Umowa

powierzenia przetwarzania danych osobowych

zawarta pomiędzy:

Narodowym Instytutem Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. med. Eleonory Reicher z siedzibą w Warszawie, ul. Spartańska 1, 02-637 Warszawa, wpisanym do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem 0000066382, NIP: 525-001-10-42, REGON: 000288567 (NIGRiR), reprezentowanym przez:

……

……

zwanym dalej **„Administratorem”**

a

……

……

zwanym dalej „**Podmiotem przetwarzającym”.**

§ 1.
Powierzenie

1. Przetwarzanie danych osobowych następuje zgodnie z obowiązującymi przepisami prawa, w tym zgodnie z przepisami 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 [Dz. Urz. UE L 119 z 4 maja 2016]), zwanego dalej „RODO”.
2. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych, a Podmiot przetwarzający przyjmuje do przetwarzania dane osobowe zgodnie z poleceniami i wskazówkami Administratora, obowiązującym prawem, w szczególności RODO, UODO oraz na warunkach określonych w umowie.
3. Jeśli w umowie użyto terminów zdefiniowanych w RODO, terminy te mają takie samo znaczenie jak w RODO, z zastrzeżeniem ust. 4.
4. Ilekroć w dalszej części umowy jest mowa o „danych osobowych” bez bliższego określenia - rozumie się przez to dane osobowe objęte umową.
5. W razie sprzeczności między postanowieniami dotyczącymi powierzenia przetwarzania danych a postanowieniami umowy głównej, pierwszeństwo w zakresie ochrony danych osobowych mają postanowienia umowy powierzenia.
6. Dla uniknięcia wątpliwości Strony uzgadniają, że:

1) Podmiot przetwarzający nie może przetwarzać danych osobowych dla żadnych innych celów niż określone w Umowie; w przypadku gdy Podmiot przetwarzający będzie przetwarzał dane osobowe w innych celach, będzie w tym zakresie pozostawał ich odrębnym administratorem;
2) Umowa nie upoważnia Podmiotu przetwarzającego do przetwarzania danych w sposób lub w zakresie niezgodnym z umową główną;
3) Podmiot przetwarzający nie decyduje o celach i sposobach przetwarzania danych osobowych.

7. Podmiot przetwarzający zobowiązuje się na bieżąco śledzić zmiany regulacji prawnych dotyczących ochrony danych osobowych i dostosowywać sposób przetwarzania danych, w szczególności procedury wewnętrzne i sposoby zabezpieczania danych osobowych do aktualnych wymagań prawnych.

§ 2.
Opis i bezpieczeństwo przetwarzania

1. Szczegóły dotyczące przetwarzania, w szczególności kategorie danych osobowych oraz cele, dla których dane osobowe są przetwarzane w imieniu Administratora, określone zostały w załączniku nr 1 do umowy powierzenia.
2. Minimalne środki techniczne i organizacyjne, jakie Podmiot przetwarzający zobowiązany jest wdrożyć w celu zapewnienia bezpieczeństwa danych, określa załącznik nr 2 do umowy powierzenia.

§ 3.
Ograniczenie przetwarzania

Podmiot przetwarzający upoważniony jest do przetwarzania, w imieniu Administratora, danych osobowych pacjentów oraz personelu Administratora wyłącznie w zakresie celów, o których mowa w załączniku nr 1 do umowy.

§ 4.
Polecenia

1. Przetwarzanie danych osobowych przez Podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakładają na niego obowiązujące przepisy prawa. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny.
2. Strony uzgadniają, że za udokumentowane polecenie uznaje się w szczególności zadania i czynności zlecone do wykonywania Przetwarzającemu dane w umowie głównej, umowie powierzenia oraz w ramach ich wykonywania.
3. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych; polecenia te są zawsze dokumentowane – strony przyjmują, że polecenia będą wydawane co najmniej w formie dokumentowej (np. za pośrednictwem korespondencji mailowej).
4. Podmiot przetwarzający bezzwłocznie powiadamia Administratora, jeżeli w opinii Podmiotu przetwarzającego polecenie wydane przez Administratora narusza obowiązujące przepisy o ochronie danych.

§ 5.
Osoby upoważnione do przetwarzania danych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, o którym mowa w art. 29 RODO, oraz przeszkolone z zakresu przepisów dotyczących ochrony danych osobowych.
2. Podmiot przetwarzający oświadcza, że każda osoba upoważniona zgodnie z ust. 1 zostanie zobowiązana do zachowania danych osobowych w tajemnicy przed ich udostępnieniem oraz do zachowania w tajemnicy wszelkich informacji dotyczących sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych przez okres trwania umowy, jak i po jej zakończeniu.
3. Podmiot przetwarzający zobowiązuje się do prowadzenia ewidencji osób upoważnionych przez niego do przetwarzania danych osobowych, zgodnie z wymaganiami określonymi w RODO.

§ 6.
Podmioty podprzetwarzające

1. Podmiot przetwarzający ma ogólną zgodę Administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do wykazu stanowiącego załącznik nr 3 do umowy powierzenia.
2. Wszelkie zmiany w wykazie, o którym mowa w ust. 1, wymagają uprzedniej pisemnej zgody Administratora.
3. Jeśli Administrator, w celu dokonania oceny zaproponowanej zmiany w wykazie, o której mowa w ust. 2, zgłosi Podmiotowi przetwarzającemu żądanie dostarczenia dodatkowej dokumentacji lub informacji dotyczących zmian, Podmiot przetwarzający zobowiązany jest do ich niezwłocznego uzupełnienia.
4. Jeżeli Podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania, dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na Podmiot przetwarzający dane zgodnie z niniejszą umową. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega Podmiot przetwarzający.
5. Na wniosek Administratora Podmiot przetwarzający przekazuje Administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje Administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, Podmiot przetwarzający może w stosownym zakresie utajnić tekst umowy przed jej udostępnieniem.
6. Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed Administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia Administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.
7. Podmiot przetwarzający zobowiązany jest do uzgodnienia z podmiotem podprzetwarzającym klauzuli dotyczącej beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą - jeżeli Podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny - Administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

§ 7.
Współpraca z Administratorem

1. Podmiot przetwarzający niezwłocznie, nie dłużej jednak niż w terminie 7 dni od otrzymania wniosku, zawiadamia Administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą.
2. Podmiot przetwarzający nie odpowiada na wniosek osoby, której dane dotyczą, samodzielnie, chyba że Administrator wyraził na to zgodę.

3. Podmiot przetwarzający pomaga Administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania.
4. Wypełniając swoje obowiązki zgodnie z ust. 1-3, Podmiot przetwarzający stosuje się do poleceń Administratora.
5. Ponadto Podmiot przetwarzający pomaga Administratorowi w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje Podmiot przetwarzający:
   1) obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych ("ocena skutków dla ochrony danych"), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
   2) obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu jego ograniczenia;
   3) obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie Administratora, jeżeli Podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;
   4) obowiązki określone w art. 32 RODO.

§ 8.
Zgłaszanie naruszeń

1. W przypadku naruszenia ochrony danych dotyczącego danych przetwarzanych przez Administratora – Podmiot przetwarzający wspomaga Administratora:
   1) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu niezwłocznie po tym, jak Administrator dowiedział się o naruszeniu, w stosownych przypadkach;
   2) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO powinny być zawarte w zgłoszeniu Administratora i obejmować co najmniej:
      a) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
      b) możliwe konsekwencje naruszenia ochrony danych osobowych;
      c) środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków

      - jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;
   3) przy wypełnianiu - zgodnie z art. 34 RODO - obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
2. W przypadku naruszenia ochrony danych dotyczącego danych przetwarzanych przez Podmiot przetwarzający – Podmiot przetwarzający zobowiązuje się niezwłocznie, nie później jednak niż w ciągu 12 godzin, powiadomić Administratora o wszelkich stwierdzonych przypadkach naruszenia ochrony danych osobowych, tj. przypadkach naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

5. Podmiot przetwarzający powiadamia Administratora o naruszeniu ochrony danych osobowych w postaci elektronicznej na wskazany przez Administratora adres e-mail. Informacja przekazana przez Podmiot przetwarzający powinna być przesłana w formie zaszyfrowanej oraz zawierać co najmniej:
   1) opis charakteru naruszenia oraz wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone oraz ilość i rodzaj danych, których naruszenie dotyczy;
   2) imię, nazwisko i dane kontaktowe inspektora ochrony danych lub innej jednostki lub osoby, z którą Administrator może się kontaktować w związku z wystąpieniem naruszenia,
   3) opis możliwych konsekwencji naruszenia;
   4) opis zastosowanych lub proponowanych do zastosowania przez Podmiot przetwarzający środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§ 9.
Postępowanie z danymi po rozwiązaniu umowy

1. Podmiot przetwarzający jest zobowiązany, adekwatnie do żądania Administratora, do zwrotu Administratorowi danych osobowych, w tym wszelkich ich kopii, w przypadku rozwiązania Umowy lub do usunięcia wszystkich danych osobowych, w terminie 7 dni roboczych od otrzymania takiego polecenia od Administratora.
2. Zwrot lub usunięcie danych osobowych nastąpi w formie i na zasadach, które określi Administrator.
3. Usunięcie danych osobowych, o którym mowa w ust. 1, należy rozumieć jako co najmniej zmodyfikowanie ich w taki sposób, aby niemożliwe było ustalenie tożsamości osoby, której dane osobowe dotyczą.
4. Podmiot przetwarzający przedstawi protokół z usunięcia danych osobowych w terminie 7 dni od dnia usunięcia danych osobowych pod rygorem zapłaty kary umownej w wysokości 200 zł za każdy rozpoczęty dzień zwłoki w przedstawieniu takiego protokołu.
5. W przypadku gdy na mocy odpowiednich przepisów prawa, Podmiot przetwarzający obowiązany będzie do przechowywania powierzonych danych osobowych po zakończeniu okresu obowiązywania umowy, Podmiot przetwarzający niezwłocznie poinformuje Administratora o wystąpieniu takich okoliczności. W powyższej sytuacji Podmiot przetwarzający uprawniony będzie do przetwarzania powierzonych danych osobowych wyłącznie w zakresie i celu wykonania takich obowiązków wynikających z przepisów prawa, zaś po ich spełnieniu niezwłocznie usunie powierzone dane osobowe. Podmiot przetwarzający zapewni przestrzeganie niniejszej umowy do czasu usunięcia lub zwrotu danych. Postanowienie ust. 4 stosuje się odpowiednio.

§ 10.
Zgodność przetwarzania

1. Podmiot przetwarzający zobowiązany jest do udzielania Administratorowi wszelkich informacji niezbędnych dla wykazania przez Administratora wywiązywania się ze wszystkich obowiązków określonych w Umowie oraz przepisach prawa, w szczególności RODO.
2. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających z RODO oraz umowy, w szczególności poprzez:
   1) prawo żądania udzielenia pisemnej informacji lub wyjaśnień przez Podmiot przetwarzający;
   2) w uzasadnionych wypadkach, dostęp do wszelkich pomieszczeń, w których Podmiot przetwarzający przetwarza dane osobowe;
   3) udostępnienie dokumentów, infrastruktury teleinformatycznej oraz systemów IT, jeżeli mają one związek z przetwarzanymi danymi osobowymi.

3. Realizacja żądań Administrator, o których mowa w ust. 2, następuje niezwłocznie, nie później jednak niż w terminie 7 dni od przedstawienia żądania pod rygorem kary umownej w wysokości 200 zł za każdy rozpoczęty dzień zwłoki w spełnieniu żądania.
4. Administrator uprawniony jest do kontroli, czy Podmiot przetwarzający przestrzega zasad przetwarzania danych osobowych, w szczególności przedstawiciele Administratora są uprawnieni do żądania od przedstawicieli Podmiotu przetwarzającego udzielenia niezbędnych informacji dotyczących sposobu, w jaki Podmiot przetwarzający przetwarza dane osobowe powierzone na podstawie umowy.
5. Kontrola przestrzegania zasad przetwarzania danych osobowych może nastąpić wyłącznie po uprzednim powiadomieniu Podmiotu przetwarzającego przez Administratora o zamiarze przeprowadzenia takiej kontroli, z co najmniej siedmiodniowym wyprzedzeniem, przed datą rozpoczęcia kontroli, ze wskazaniem w formie pisemnej osób wyznaczonych do przeprowadzenia kontroli.
6. Na skutek przeprowadzonej kontroli, Administrator może skierować do Podmiotu przetwarzającego polecenia dotyczące przetwarzania danych osobowych, które Podmiot przetwarzający jest zobowiązany zastosować niezwłocznie, ale nie później niż w terminie 14 dni od uzyskania polecenia Administratora pod rygorem kary umownej w wysokości 200 zł za każdy rozpoczęty dzień zwłoki w realizacji polecenia. O sposobie wdrożenia poleceń Podmiot przetwarzający informuje Administratora.
7. Na żądanie Administratora, Podmiot przetwarzający powinien w szczególności niezwłocznie poinformować Administratora o miejscach, w których przetwarzane są dane osobowe, wykazie osób upoważnionych do przetwarzania danych osobowych oraz udzielić mu innych informacji niezbędnych do zrealizowania obowiązków wynikających z RODO, np. na temat środków technicznych i organizacyjnych podjętych przez Podmiot przetwarzający.
8. Kontrole Administrator przeprowadza w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Jeśli kontrola wykaże co najmniej 3 nieprawidłowości w przetwarzaniu danych osobowych, koszt jej przeprowadzenia pokrywa Podmiot przetwarzający.
9. Ponadto, w przypadku gdy Podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszej umowy, Administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy Podmiot przetwarzający zapewni zgodność z niniejszą umową. Podmiot przetwarzający niezwłocznie zawiadamia Administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszej umowy.

§ 11.
Transfery danych osobowych

1. Podmiot przetwarzający gwarantuje, że żadne przetwarzane przez niego dane osobowe nie będą transferowane do państw trzecich w rozumieniu RODO.
2. Podmiot przetwarzający jest uprawniony do transferowania danych osobowych do państw trzecich w rozumieniu RODO wyłącznie pod warunkiem wcześniejszego uzyskania zgody Administratora.

§ 12.
Zwolnienie z odpowiedzialności

1. W przypadku gdy w związku z naruszeniem przez Podmiot przetwarzający jakichkolwiek przepisów dotyczących ochrony danych osobowych lub postanowień niniejszej umowy, niezależnie od tego, czy naruszenie jest zawinione, Administrator poniesie jakiekolwiek koszty, w szczególności kary pieniężne lub odszkodowania na rzecz osób, których dane osobowe przetwarzane są na podstawie

umowy, organów nadzorczych lub jakichkolwiek innych podmiotów, oraz koszty obsługi prawnej tych żądań, Podmiot przetwarzający zwolni Administratora z odpowiedzialności wobec tych osób, organów i podmiotów z tytułu jakiejkolwiek szkody poniesionej w związku z takim naruszeniem przez Podmiot przetwarzający oraz zobowiązany będzie do przejęcia obowiązku zapłaty tych kosztów w pełnej wysokości.

2. W przypadku gdy w związku z naruszeniem, o którym mowa w ust. 1, wytoczone zostanie postępowanie sądowe lub będzie prowadzone postępowanie przez organ nadzorczy – Podmiot przetwarzający zobowiązuje się do udzielenia Administratorowi wszelkiego wsparcia w takim postępowaniu, a także do przejęcia odpowiedzialności w przypadku przyznania podmiotowi danych lub innemu właściwemu podmiotowi odszkodowania w takim postępowaniu, w wysokości odpowiadającej równowartości przyznanego odszkodowania oraz wszelkich kosztów poniesionych przez Administratora w takim postępowaniu.
3. Podmiot przetwarzający zobowiązuje się do niezwłocznego, nie później niż w terminie 3 dni od dnia powzięcia stosownej wiedzy, poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych, o jakiejkolwiek decyzji administracyjnej 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 UODO.
4. Podmiot przetwarzający zobowiązany jest na żądanie Administratora do przekazania mu wszelkich informacji dotyczących zakresu, wyników oraz działań podjętych przez uprawniony organ w wyniku przeprowadzonej kontroli lub w prowadzonym postępowaniu, w szczególności administracyjnym lub sądowym. Powyższe dotyczy wyłącznie danych osobowych powierzonych Podmiotowi przetwarzającemu przez Administratora.
5. Do kar umownych wskazanych w umowie powierzenia odpowiednie zastosowanie znajdą postanowienia umowy głównej dotyczące kar umownych.

§ 13.
Obowiązywanie i rozwiązanie umowy

1. Umowa obowiązuje przez czas trwania umowy głównej, tj. od dnia _____ do dnia _____.
2. Administrator upoważniony jest do rozwiązania umowy ze skutkiem natychmiastowym, w przypadku, gdy:
   1) organy administracji publicznej odpowiedzialne za nadzór nad przetwarzaniem danych osobowych wykażą, że Podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych;
   2) Administrator stwierdzi, w tym po przeprowadzeniu kontroli, że Podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych określonych w RODO lub umowie;
   3) Podmiot przetwarzający uniemożliwia lub utrudnia przeprowadzenie kontroli, o której mowa w § 10;
   4) Administrator zawiesił przetwarzanie danych osobowych przez Podmiot przetwarzający i zgodność z niniejszą umową nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
   5) Podmiot przetwarzający poważnie lub stale narusza niniejszą umowę lub obowiązki wynikające z przepisów;

6) Podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub organu nadzorczego.

3. W celu uniknięcia wątpliwości strony potwierdzają, że:
   1) z tytułu przetwarzania danych osobowych Podmiotowi przetwarzającemu nie przysługuje odrębne wynagrodzenie;
   2) Podmiot przetwarzający jest zobowiązany do stosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczne przetwarzanie danych osobowych oraz do wdrażania wszelkich zaleceń i poleceń Administratora na swój koszt.

§ 14.
Postanowienia końcowe

W sprawach nieuregulowanych w umowie powierzenia odpowiednie zastosowanie znajdą postanowienia umowy głównej.

Załączniki:

1) Szczegóły dotyczące operacji przetwarzania;

2) Minimalne środki techniczne i organizacyjne;

3) Wykaz podmiotów podprzetwarzających

Podmiot przetwarzający	**Administrator**
Podpis:_____	*Podpis*: _____

Załącznik nr 1

Szczegóły dotyczące operacji przetwarzania

1. Kategorie osób, których dane osobowe są przetwarzane, oraz kategorie przetwarzanych danych osobowych:

Lp.	Kategoria osób, których dane dotyczą	Kategorie przetwarzanych danych osobowych
1.	Pacjenci	dane zwykłe (imię i nazwisko, adres zamieszkania, PESEL, dane do kontaktu) oraz dane szczególnej kategorii (dane dotyczące zdrowia) – zawarte w dokumentacji medycznej pacjentów
2.	Osoby udzielające świadczeń zdrowotnych	dane zwykłe (imię i nazwisko, stopień/tytuł naukowy, specjalizacje, NPWZ, stanowisko, miejsce zatrudnienia)

2. Charakter przetwarzania

Regularny dostęp do danych, determinowany potrzebami związanymi z udzielaniem świadczeń zdrowotnych w zakresie teleradiologii.

3. Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora

Podmiot przetwarzający może przetwarzać dane osobowe wyłącznie w celu wykonania postanowień umowy głównej.

4. Czas trwania przetwarzania

Czas obowiązywania umowy głównej.

5. Przedmiot przetwarzania

Na danych osobowych, o których mowa w ust. 1, wykonywane będą w ww. celach i czasie, w sposób niezautomatyzowany, operacje polegające w szczególności na:

1) utrwalaniu;
2) organizowaniu;
3) przechowywaniu;
4) adaptowaniu lub modyfikowaniu;
5) pobieraniu;
6) przeglądaniu;
7) wykorzystywaniu.

Załącznik nr 2

Minimalne środki techniczne i organizacyjne

1. Wykaz stosowanych przez Podmiot przetwarzający zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji

1) ……. ;

2) ……. ;

3) ……. .

2. Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych

☒	Odpowiednio szyfrowana transmisja danych elektronicznych zgodnie z aktualnym stanem techniki

3. Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania

☒	Pracownicy muszą przechodzić regularne szkolenia z zakresu ochrony danych i bezpieczeństwa informacji
☒	Wyznaczenie personelu administracyjnego odpowiedzialnego za zarządzanie hasłami.
☒	Pracownicy są wyraźnie zobowiązani do zachowania tajemnicy
☒	Przekazywanie danych osobowych do prywatnych urządzeń końcowych lub systemów jest zabronione z technicznego i/lub organizacyjnego punktu widzenia

4. Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

☒	Polityka tworzenia kopii zapasowych i odzyskiwania, która obejmuje również zrozumiałe ćwiczenia odzyskiwania, zgodna z najwyższymi aktualnymi standardami
☒	Istnieje plan awaryjnego działania na wypadek utraty dostępu do danych, który jest regularnie testowany

5. Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

☒	Regularne wyrywkowe kontrole systemów IT
☒	Regularny audyt fizycznych praw dostępu

6. Środki umożliwiające identyfikację i autoryzację użytkowników

☒	Polityka autoryzacji rozróżnia co najmniej uprawnienia do odczytu i zapisu

☒	Polityka autoryzacji zapewnia, że dostęp do danych mają wyłącznie upoważnione osoby i tylko w zakresie niezbędnym
☒	Dostęp do systemów informatycznych zapewniony jest z odpowiednim zabezpieczeniem hasłem, współmiernym do wrażliwości przetwarzanych danych
☒	Uwierzytelnianie dwuskładnikowe w celu uzyskania dostępu do wrażliwych danych osobowych przechowywanych elektronicznie na mobilnych nośnikach danych lub do danych osobowych zidentyfikowanych jako wymagające szczególnej ochrony

7. Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe

☒	Instrukcje stanowiące, że wyświetlacze danych mają być chronione przed oglądaniem przez osoby nieupoważnione oraz że stacja robocza ma być zamknięta dla osób nieupoważnionych za pomocą zabezpieczonej hasłem blokady ekranu
☒	Odpowiednia ochrona wizualna plików i dokumentów, a także monitorów, które można łatwo przeglądać
☒	Przechowywanie nośników danych zawierających dane osobowe odbywa się w zamykanych na klucz, odpornych na zniszczenie szafach/obiektach z udokumentowanym przydziałem kluczy
☒	Zainstalowane system(-y) alarmowy(-e) w obszarach istotnych dla usługi kontraktowej
☒	Zamki bezpieczeństwa w obszarach istotnych dla usługi kontraktowej
☒	Usługi pracowników ochrony w obszarach istotnych dla usługi kontraktowej
☒	Instrukcje dotyczące zamykania pomieszczeń podczas nieobecności

8. Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT

☒	Korzystanie z najnowocześniejszego oprogramowania ochronnego (np. rozwiązań chroniących przed złośliwym oprogramowaniem, zapór sieciowych itp.)
☒	System alarmowy w przypadku (próby) nieuprawnionego dostępu do danych elektronicznych

9. Środki zapewniające minimalizację danych

☐	Instrukcja usuwania danych, które nie są już potrzebne

10. Środki zapewniające odpowiednią jakość danych

☒	Jeśli pliki w systemach elektronicznego przetwarzania danych zostaną zmienione lub usunięte, zostanie to zarejestrowane
☒	Wyklucza się wprowadzanie danych przez osoby nieupoważnione

11. Środki zapewniające rozliczalność

☒	Istnieje stale aktualizowana polityka uprawnień, która zapewnia, że tylko pracownicy mają dostęp do danych wymaganych do wykonywania swoich obowiązków i tylko w zakresie niezbędnym w każdym przypadku
☒	Sformalizowany dobór procesora
☒	Polityka haseł i jej techniczne wdrożenie/egzekwowanie
☒	Prowadzenie rejestru czynności przetwarzania
☒	Wyznaczenie inspektora ochrony danych
☒	Zniszczenie nośników danych i danych jest rejestrowane
☒	Uporządkowany proces przyznawania i odbierania fizycznych praw dostępu

12. Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy administratorowi

☒	Administrator musi zostać poinformowany w odpowiednim czasie o incydentach związanych z ochroną danych lub bezpieczeństwem informacji. Podejrzenia o naruszeniu należy również niezwłocznie zgłaszać.
☒	Wytyczne/instrukcje dotyczące postępowania w przypadku naruszeń ochrony danych podlegających zgłoszeniu
☒	Zarządzanie reagowaniem na incydenty, w tym funkcje alarmowe i ostrzegawcze; określenie środków, obowiązków i procesów minimalizacji szkód, a także obowiązków sprawozdawczych wobec organu nadzorczego i osób, których dane dotyczą

Załącznik nr 3

Wykaz podmiotów podprzetwarzających