

Załącznik nr ... do
Umowy nr ... z dnia

.....

Umowa powierzenia przetwarzania danych osobowych
zwana dalej „Umową”
zawarta w dniu r. w Łodzi pomiędzy:

Instytutem Medycyny Pracy imienia prof. dra med. Jerzego Nofera z siedzibą w Łodzi przy ulicy św. Teresy od Dzieciątka Jezus 8, NIP 7240003125, REGON 000288538, wpisanym do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Łodzi – Śródmieścia w Łodzi, XX Wydział Krajowego Rejestru Sądowego pod nr KRS 0000011997, zwanym dalej „Zamawiającym” lub „Administratorem”, reprezentowanym przez:

1) Prof. dr hab. med. Jolantę Walusiak-Skorupę – Dyrektora Instytut

a

.....

zwaną dalej „Wykonawcą” lub „Podmiotem przetwarzającym”

Definicje

Użyte w niniejszej umowie określenia:

- 1) **Ustawa** – oznacza ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781¹);
- 2) **Umowa główna** - umowa zawarta między Zamawiającym a Wykonawcą na budowę i wdrożenie e-Uслуг dla Zamawiającego oraz ich integracji z Oprogramowaniem Zamawiającego , w ramach Projektu pn. „Wprowadzenie nowoczesnych e-Uслуг w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia”;
- 3) **RODO** – oznacza 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);
- 4) **dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), powierzone do dalszego przetwarzania w związku z realizacją Umowy głównej,
- 5) **możliwa do zidentyfikowania osoba fizyczna** – oznacza osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

¹ Należy wypełnić

- 6) **Administrator** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
- 7) **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora na podstawie Umowy. Podmiotem przetwarzającym jest Wykonawca w rozumieniu Umowy Głównej;
- 8) **podprocesor** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu powierzono dane przez Podmiot przetwarzający w imieniu Administratora;
- 9) **pracownik Podmiotu przetwarzającego** – oznacza osobę zatrudnioną na umowę o pracę, umowy o świadczenie usług oraz inną osobę fizyczną, niezależnie od podstawy współpracy z Podmiotem przetwarzającym, za pomocą których Podmiot przetwarzający realizuje Umowę główną;
- 10) **przetwarzanie** – 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; w zakresie niezbędnym do realizacji umowy;
- 11) **naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 1.

Powierzenie przetwarzania danych osobowych

1. Zamawiający będący Administratorem powierza Wykonawcy będącym Podmiotem przetwarzającym przetwarzanie danych osobowych znajdujących się w systemach teleinformatycznych wykorzystywanych przez Administratora, do których dostęp Podmiot przetwarzający uzyska w związku z realizacją Umowy głównej.
2. Podmiot przetwarzający niniejszym oświadcza, iż:
 - a) są mu znane wszelkie obowiązki nałożone przez przepisy ustawy o ochronie danych osobowych oraz RODO, na podmiot przetwarzający dane osobowe powierzone mu do przetwarzania przez Administratora, a w szczególności treść art. 28 RODO,
 - b) dysponuje odpowiednimi środkami oraz stosuje je, w tym należyтыми zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami ustawy o ochronie danych osobowych oraz RODO,
 - c) przygotował i wdrożył stosowne polityki ochrony danych osobowych wymagane od podmiotu, któremu powierzono przetwarzanie danych osobowych, zgodnie z postanowieniami ustawy o ochronie danych osobowych oraz RODO,
 - d) zapewnia gwarancję wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których przetwarzane na podstawie Umowy dane dotyczą.

3. Podmiot przetwarzający jest podmiotem przetwarzającym dane na zlecenie w rozumieniu art. 28 RODO.

§ 2.

Cel przetwarzania danych osobowych oraz rodzaj i kategoria osób, których dane dotyczą

1. Podmiot przetwarzający nie decyduje o celach i środkach przetwarzania powierzonych danych osobowych.
2. Podmiot przetwarzający może przetwarzać następujące dane osobowe gromadzone za pomocą oprogramowania wykorzystywanego przez Zamawiającego wyłącznie w celu związanym z realizacją Umowy głównej, w szczególności:
 - 1) dane osobowe pacjentów Administratora, w zakresie: imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, PESEL, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, nr telefonu i adres poczty elektronicznej, dane dotyczące przedstawiciela ustawowego, pełnomocnika lub opiekuna prawnego i faktycznego - dane osobowe zwykłe, dane dotyczące stanu zdrowia - dane osobowe szczególnej kategorii.
 - 2) dane osobowe personelu medycznego Administratora w zakresie; imię i nazwisko lekarza kierującego, tytuł zawodowy, uzyskane specjalizacje, nr prawa wykonywania zawodu - dane osobowe zwykłe.
 - 3) dane osobowe personelu administracyjnego Administratora, odpowiedzialnego za realizację przedmiotu Umowy głównej (w postaci; imię i nazwisko, służbowe dane kontaktowe - dane osobowe zwykłe.
3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji przedmiotu Umowy głównej.
4. Podmiot przetwarzający zapewni, że przetwarzanie danych osobowych przez niego i jego podprocesorów będzie odbywało się wyłącznie na terytorium UE.

§ 3.

Dalsze powierzenie danych osobowych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych:
2. W celu uzyskania zgody Administratora, Podmiot przetwarzający informuje go w szczególności o:
 - 1) firmie, adresie siedziby tego podmiotu oraz jego danych kontaktowych,
 - 2) miejscu przetwarzania przez ten podmiot danych osobowych,
 - 3) planowanym terminie rozpoczęcia powierzenia przetwarzania danych osobowych przez ten podmiot.
3. W każdym przypadku dalszego powierzenia przetwarzania danych osobowych, Wykonawca ma obowiązek niezwłocznie przekazać Zamawiającemu informacje o dacie zawarcia umowy dalszego powierzenia przetwarzania danych osobowych, firmie, adresie siedziby podprocesora oraz adresie rzeczywistego przetwarzania danych osobowych przez podprocesora. W przypadku jakichkolwiek zmian w zakresie wykorzystywanych podprocesorów, miejsca przetwarzania przez nich danych osobowych, ich danych identyfikacyjnych lub kontaktowych, Wykonawca jest zobowiązany niezwłocznie poinformować o nich Zamawiającego.

3. Administrator nie wyraża zgody na przetwarzanie powierzonych danych w Stanach Zjednoczonych.
4. Przekazanie powierzonych danych do innych niż Stany Zjednoczone państw trzecich, może nastąpić jedynie na pisemne polecenie Administratora danych, po spełnieniu gwarancji, że ustawodawstwo tego kraju jest zgodne z wymogami wskazanymi przez Trybunału Sprawiedliwości Unii Europejskiej (TSUE) oraz z równoważnym stopniem ochrony danych osobowych zapewnianym w EOG - chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny
3. Zamawiający może wycofać zgodę na dalsze powierzenie przetwarzania danych osobowych podprocesorom, jeśli z okoliczności wynika, że przetwarzanie przez nich danych osobowych odbywa się niezgodnie z prawem, Umową lub zagraża bezpieczeństwu danych osobowych. W przypadku wycofania zgody, Wykonawca jest zobowiązany niezwłocznie doprowadzić do zaprzestania przetwarzania danych przez podprocesora.
4. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za działania i zaniechania swoich podprocesorów jak za własne. W przypadku gdyby w wyniku działania lub zaniechania podwykonawcy, Zamawiający poniósł szkodę, Wykonawca zobowiązuje się do jej naprawienia.

§ 4.

Zadania i obowiązki podmiotu przetwarzającego

1. Przy przetwarzaniu danych osobowych Podmiot przetwarzający przestrzega zasad wskazanych w Umowie, w ustawie o ochronie danych osobowych oraz w RODO.
2. Podmiot przetwarzający oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych oraz spełnia wymagania określone w przepisach ustawy o ochronie danych osobowych oraz RODO, a także podejmie środki zabezpieczające powierzone dane przed rozpoczęciem przetwarzania danych osobowych zapewniające adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
3. W przypadku dalszego powierzenia przez Podmiot przetwarzający przetwarzania danych osobowych zgodnie z § 3 Umowy, postanowienia ust. 1 i 2 znajdują zastosowanie również odnośnie do osób lub podmiotów wskazanych w § 3, przy czym za ich realizację przez osoby lub podmioty wskazane w § 3 odpowiada również Podmiot przetwarzający, jak za własne działania lub zaniechania.
4. W przypadku, gdyby w toku realizacji Umowy, doszło do zmian wymagań prawnych związanych z przetwarzaniem danych osobowych w szczególności wymagań dotyczących zabezpieczenia danych osobowych, Podmiot przetwarzający zobowiązany jest własnym kosztem i staraniem do zapewnienia przetwarzania danych osobowych, w tym ich zabezpieczenia w sposób zgodny z przepisami prawa polskiego.
5. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy Podmiotu przetwarzającego posiadający imienne upoważnienie do przetwarzania danych osobowych związanych z realizacją Umowy. Upoważnienie wygasa z chwilą ustania zatrudnienia upoważnionego pracownika lub odwołania upoważnienia.
6. Administrator umocowuje Podmiot przetwarzający do wydawania i odwoływania pracownikom Podmiotu przetwarzającego imiennych upoważnień do przetwarzania danych osobowych. Upoważnienia przechowuje Podmiot przetwarzający w swojej siedzibie. Podmiot przetwarzający każdorazowo niezwłocznie, nie później niż w ciągu następnego dnia roboczego, informuje Administratora o imieniu i

nazwisku osoby, którą upoważnił do przetwarzania danych osobowych oraz jej roli w realizacji przedmiotu Umowy głównej. Do odwołania upoważnienia stosuje się zdanie poprzedzające.

7. Administrator uprawniony jest do zgłoszenia sprzeciwu wobec upoważnienia osób, których upoważnił Podmiot przetwarzający do przetwarzania danych. W takim przypadku Podmiot przetwarzający niezwłocznie odwołuje takie upoważnienie i informuje o tym Administratora.
8. Podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z wymaganiami art. 30 ust 2 RODO i poinformuje o tym Administratora.
9. Podmiot przetwarzający zobowiązuje się do szczególnej ochrony przekazanych mu do przetwarzania przez Administratora danych oraz do nieprzekazywania ich osobom nieuprawnionym i nieupoważnionym do przetwarzania.
10. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne informacje, zapewni pomoc Administratorowi w wywiązaniu się z obowiązków określonych w RODO, w tym pomoże Administratorowi wywiązać się z obowiązku odpowiadania na żądanie osoby, której dane dotyczą, w zakresie wykonywania jej praw oraz obowiązków określonych w art. 32-36 RODO.
11. W sytuacji awaryjnej Podmiot przetwarzający otrzymuje zdalny dostęp terminalowy za pośrednictwem VPN po uprzednich konsultacjach z działem IT Administratora.

§ 5.

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do bezwzględnego zachowania w poufności wszelkich informacji oraz danych osobowych, jak również sposobu ich zabezpieczenia, powierzonych mu w trakcie obowiązywania Umowy lub uzyskanych w związku z wykonywaniem czynności objętych Umową, także po wygaśnięciu Umowy. Obowiązek ten nie dotyczy informacji, co do których Administrator ma nałożony ustawowy obowiązek publikacji, które stanowią informacje publiczną lub które zostały opublikowane przez Administratora. Do obowiązku zachowania poufności przez Podmiot przetwarzający stosuje się § 15 Umowy głównej.
2. Podmiot przetwarzający zobowiąże swoich pracowników i będzie od nich wymagał bezwzględnego zachowania wszelkich informacji oraz danych osobowych, a także sposobu ich zabezpieczenia w poufności, zarówno w trakcie obowiązywania Umowy, jak również po jej wygaśnięciu.

§ 6.

Prawo kontroli

1. Administrator uprawniony jest do żądania od Podmiotu przetwarzającego wyjaśnień dotyczących:
 - 1) stosowanych przez Podmiot przetwarzający środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w tym stosowanych środków sprzętowych i programowych,
 - 2) przetwarzania powierzonych danych osobowych.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego informowania Administratora o wszelkich przypadkach naruszenia bezpieczeństwa oraz tajemnicy danych osobowych lub ich niewłaściwym użyciu, a także o wszelkich czynnościach związanych z Umową, prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych, urzędy publiczne, policję lub sądy.

3. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin na adres: iod@imp.lodz.pl.
4. W przypadku wystąpienia okoliczności, o których mowa w ust. 2 i 3, Podmiot przetwarzający jest zobowiązany do podjęcia środków zabezpieczających dane osobowe.
5. Podmiot przetwarzający zobowiązuje się do (zgodnie z art. 28 ust. 3 lit h) RODO):
 - 1) umożliwienia Administratorowi dokonania audytu w miejscach, w których są przetwarzane powierzone dane osobowe, w zakresie stosowania Umowy, w terminie ustalonym przez Strony nie później jednak niż 5 dni od dnia powiadomienia Podmiotu przetwarzającego przez Administratora o zamiarze przeprowadzenia audytu, w celu sprawdzenia prawidłowości przetwarzania oraz zabezpieczania danych osobowych,
 - 2) w przypadku powzięcia przez Administratora wiadomości o rażącym naruszeniu przez Podmiot przetwarzający zobowiązań wynikających z ustawy o ochronie danych osobowych, RODO lub Umowie, Podmiot przetwarzający umożliwi Administratorowi dokonanie niezapowiedzianego audytu,
 - 3) zastosowania się do zaleceń poaudytowych Administratora, dotyczących poprawy jakości zabezpieczania danych osobowych oraz sposobu ich przetwarzania.

§ 7.

Usunięcie danych osobowych

1. Podmiot przetwarzający w przypadku rozwiązania Umowy głównej, odstąpienia od tej Umowy lub jej wygaśnięcia, jeżeli odrębne przepisy powszechnie obowiązującego prawa nie nakazują ich dalszego przechowywania, trwale zniszczy wszystkie powierzone mu do przetwarzania dane osobowe na podstawie Umowy i ich kopie. Podmiot przetwarzający przedstawi Administratorowi oświadczenie potwierdzające zniszczenie danych.
2. Na każde wezwanie Administratora, niezależnie od obowiązku wynikającego z ust. 1, Podmiot przetwarzający zobowiązuje się zniszczyć wskazaną część przekazanych danych w terminie 5 dni od dnia wezwania oraz przedstawić oświadczenie potwierdzające ich zniszczenie.
3. Wykonawca, na żądanie Zamawiającego, zapewni dostęp do własnych urządzeń na których przetwarzane były dane osobowe, w celu sprawdzenia czy dane zostały zwrócone lub usunięte zgodnie z ust. 1 i 2.

§ 8.

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników oraz podprocesorów, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.
2. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
3. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu

przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.

§ 9.

Postanowienia końcowe

1. Umowa została zawarta na czas wykonywania Umowy głównej. Umowa wygasa z chwilą wygaśnięcia lub rozwiązania Umowy głównej.
2. Wszelkie zmiany Umowy wymagają formy pisemnej lub elektronicznej pod rygorem nieważności, w postaci Aneksu do Umowy.
3. Wszelka korespondencja związana z Umową kierowana będzie na zasadach opisanych w Umowie głównej.
4. Strony postanawiają, że wszelkie spory wynikłe w związku z zawarciem lub wykonaniem przedmiotu Umowy rozstrzygane będą przez sąd powszechny miejscowo właściwy dla siedziby Zamawiającego.
5. Umowa została zawarta w formie pisemnej/ elektronicznej² w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
6. W sprawach nieuregulowanych w Umowie stosuje się przepisy prawa polskiego, w szczególności przepisy Kodeksu cywilnego.

.....
Zamawiający

.....
Wykonawca

² Niepotrzebne wykreślić.