Umowa powierzenia przetwarzania danych osobowych
Stanowiąca załącznik nr 3 do umowy głównej z dnia …… numer…….
(zwana dalej „Umową")
Zawarta pomiędzy:

Śląskim Uniwersytetem Medycznym w Katowicach
40-055 Katowice ul. Poniatowskiego 15
Regon: 000289035
NIP: 634 000 53 01

zwanym w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

reprezentowanym przez:
1. ……
2. ……

oraz
……..
zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**
reprezentowanym przez: ……

łącznie zwanymi w dalszej części umowy **„Stronami"**

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem" lub „RODO") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot 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.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy dane *pracowników Administratora, którzy są uczestnikami szkolenia w postaci imienia i nazwiska.*
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu *realizacji umowy głównej z dnia …… nr ……*

§3
Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *zgodny z okresem obowiązywania umowy głównej z dnia:…… numer……..*
2. Każda ze Stron może wypowiedzieć niniejszą Umowę z zachowaniem 14 dniowego okresu wypowiedzenia.

§4
Obowiązki Podmiotu przetwarzającego

1. Podmiot 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.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust. 3 lit. b) Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot 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.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu w ciągu 24 h.

§5
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 lit. h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§6
Dalsze powierzenie danych 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. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych 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. Podwykonawca, o którym mowa w ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 7
Odpowiedzialność Podmiotu przetwarzającego

1. 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.
2. 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 jakiejkolwiek 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. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

3. Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Podmiocie przetwarzającym.

§8

Minimalne wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji

1. Podmiot przetwarzający będący osobą prawną opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo Podmiotu przetwarzającego warunków umożliwiających realizację i egzekwowanie następujących działań:
    a. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
    b. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
    c. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
    d. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
    e. bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w punkcie poprzedzającym;
    f. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
        i. zagrożenia bezpieczeństwa informacji,
        ii. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
        iii. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
    g. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
        i. monitorowanie dostępu do informacji,
        ii. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
        iii. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
    h. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
    i. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
    zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
    j. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
    k. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
        i. dbałości o aktualizację oprogramowania,
        ii. minimalizowaniu ryzyka utraty informacji w wyniku awarii,
        iii. ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
        iv. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
        v. zapewnieniu bezpieczeństwa plików systemowych,
        vi. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

vii. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
viii. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

l. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
m. zapewnienia okresowego audytu wewnętrznego lub innej formy kontroli lub przeglądu w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji Podmiotu przetwarzającego został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:
   a. PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
   b. PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
   c. PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
4. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych Podmiot przetwarzający ustanowi dodatkowe.

§9
Rozwiązanie Umowy

Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z Umową i RODO;
c) naruszył świadomie przepisy o ochronie danych osobowych;
d) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;
e) znacząco wzrosło ryzyko bezpieczeństwa przetwarzania powierzonych danych osobowych.

§10
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych 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. Podmiot 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.
3. W razie uzyskania informacji lub powzięcia uzasadnionych podejrzeń przez Podmiot przetwarzający, że nastąpiło ujawnienie informacji poufnych w sposób inny niż ustalony postanowieniami niniejszej Umowy, Podmiot przetwarzający zobowiązany jest do niezwłocznego poinformowania Administratora danych o tym fakcie oraz do podjęcia wszelkich pozostających w granicach możliwości działań oraz pełnej współpracy z Administratorem danych na rzecz ograniczenia i usunięcia skutków tego faktu.
4. Podmiot przetwarzający może ujawnić informacje poufne w wymaganym zakresie, o ile obowiązek ich ujawnienia wynika z przepisów prawa, lub żądania organu państwowego albo samorządowego posiadającego prawo do wnioskowania o ujawnienie takich informacji; wymagań sądu powszechnego, sądu arbitrażowego albo sądu administracyjnego w ramach toczącego się postępowania.
5. Powyższe zobowiązanie do zachowania poufności nie ma zastosowania do informacji, które:
   a. są lub staną się powszechnie dostępne w sposób inny niż poprzez naruszenie zobowiązania do zachowania poufności przez Administratora Danych,
   b. ujawniono na podstawie wcześniejszego porozumienia z Administratorem Danych,
   c. zostały opracowane w sposób niezależny, bez dostępu do lub korzystania z informacji poufnych ujawnionych przez Administratora Danych.
6. Zobowiązanie Podmiotu przetwarzającego wynikające z niniejszego paragrafu będą wiążące również po upływie okresu obowiązywania lub rozwiązaniu niniejszej Umowy.

§11

Zastrzeżenia finansowe

1. Podmiot przetwarzający nie przenosi kosztów związanych z realizacją niniejszej umowy na Administratora Danych, w szczególności wynikających z wdrażanych zabezpieczeń i działań organizacyjnych związanych z przetwarzaniem powierzonych do przetwarzania danych osobowych.
2. Pozostałe kwestie finansowe w tym kary umowne reguluje umowa główna.

§12

Postanowienia końcowe

3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
4. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia RODO oraz innych aktów prawnych powszechnie obowiązujących w zakresie bezpieczeństwa informacji, w tym w szczególności cyberbezpieczeństwa.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla Administratora danych.
6. Zmiany niniejszej Umowy wymagają zachowania formy pisemnej.

_____ _____

Administrator danych Podmiot przetwarzający