Załącznik nr 3
do Umowy
na przeprowadzenie zajęć w kursie realizowanym
w ramach kształcenia podyplomowego
– dla osób prowadzących działalność gospodarczą

Umowa powierzenia przetwarzania danych osobowych
stanowiąca załącznik nr 2 do umowy numer …… z dnia ……..
(zwana dalej „Umową") pomiędzy:

Śląskim Uniwersytetem Medycznym w Katowicach z siedzibą w Katowicach przy ul. Poniatowskiego 15, posiadającym NIP: 634-000-53-01, REGON: 000289035
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"**

PREAMBUŁA

Niniejsza umowa została opracowana na podstawie Decyzji wykonawczej Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725

SEKCJA I

Klauzula 1
Cel i zakres

a) Celem niniejszych standardowych klauzul umownych („klauzule") jest zapewnienie przestrzegania art. 28 ust. 3 i 4 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).
b) Administratorzy i podmioty przetwarzające wymienieni w załączniku I uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 lub art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.
c) Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku II.
d) Załączniki I–IV stanowią integralną część klauzul.
e) Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

f) Niniejsze klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

Klauzula 2
Niezmienność klauzul

a) Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.
b) Postanowienie to nie uniemożliwia stronom umieszczania standardowych klauzul umownych określonych w niniejszych klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami umownymi ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

Klauzula 3
Wykładnia

a) Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725, terminy te mają takie samo znaczenie jak w tych rozporządzeniach.
b) Niniejsze klauzule odczytuje się i interpretuje w świetle odpowiednio przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.
c) Niniejszych klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725 ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

Klauzula 4
Hierarchia

W razie sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszych klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

Klauzula 5 – fakultatywna
Klauzula przystąpienia

a) Każdy podmiot niebędący stroną niniejszych klauzul może za zgodą wszystkich stron przystąpić do niniejszych klauzul jako administrator lub podmiot przetwarzający w dowolnym czasie, wypełniając załączniki i podpisując załącznik I.
b) Po wypełnieniu i podpisaniu załączników wymienionych w lit. a) podmiot przystępujący jest traktowany jako strona niniejszych klauzul i ma prawa i obowiązki administratora lub podmiotu przetwarzającego, zgodnie z rolą nadaną mu w załączniku I.
c) Przed przystąpieniem do niniejszych klauzul jako ich strona podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych klauzul.

SEKCJA II

OBOWIĄZKI STRON

Klauzula 6
Opis przetwarzania

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w **załączniku II.**

Klauzula 7
Obowiązki stron

7.1. Polecenia

a) Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. 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. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.
b) Podmiot przetwarzający bezzwłocznie powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez administratora narusza rozporządzenie (UE) 2016/679 lub rozporządzenie (UE) 2018/1725 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

7.2. Ograniczenie celu

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w **załączniku II**, chyba że otrzyma dalsze polecenia od administratora.

7.3. Czas trwania przetwarzania danych osobowych

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony **w załączniku II.**

7.4. Bezpieczeństwo przetwarzania

a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.
b) Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

7.5. Dane wrażliwe

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

7.6. Dokumentacja i zgodność

a) Strony są w stanie wykazać zgodność z niniejszymi klauzulami.
b) Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.

c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.
d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
e) Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7.7.Korzystanie z usług podmiotów podprzetwarzających

a) OPCJA 1: UPRZEDNIA SZCZEGÓŁOWA ZGODA: Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu administratora zgodnie z niniejszymi klauzulami podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody co **najmniej 10 dni roboczych** przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik IV zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika IV.

   OPCJA 2: OGÓLNA PISEMNA ZGODA: Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu. Podmiot przetwarzający informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej **10 dni roboczych**, dając tym samym administratorowi wystarczająco dużo czasu na wyrażenie sprzeciwu wobec takich zmian przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego (podmiotów podprzetwarzających). Podmiot przetwarzający przekazuje administratorowi niezbędne informacje umożliwiające mu skorzystanie z prawa sprzeciwu.

b) Jeżeli podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), 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 niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych klauzul oraz rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.
c) 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 utajnić tekst umowy przed jej udostępnieniem.
d) 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.
e) Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą 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.

7.8. Międzynarodowe przekazywanie danych

a) Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.
b) Jeżeli zgodnie z klauzulą 7.7 podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 8
Pomoc dla administratora

a) Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że administrator wyraził na to zgodę.

b) 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. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.

c) Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto 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 rozporządzenia (UE) 2016/679

d) Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

Klauzula 9
Zgłaszanie naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679 lub, w stosownych przypadkach, z art. 34 i 35 rozporządzenia (UE) 2018/1725, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

9.1. Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:

a) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorczemu(-ym) niezwłocznie po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
b) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:
    1. 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;
    2. możliwe konsekwencje naruszenia ochrony danych osobowych;
    3. 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;
c) przy wypełnianiu – zgodnie z art. 34 rozporządzenia (UE) 2016/679– 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.

9.2. Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
b) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym 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.

Strony określają w załączniku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679.

SEKCJA III

POSTANOWIENIA KOŃCOWE

Klauzula 10
Naruszenie klauzul i rozwiązanie umowy

a) Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725, w przypadku gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi klauzulami,

lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych klauzul.

b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:
   1) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
   2) podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725;
   3) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

c) Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.

d) Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych klauzul do czasu usunięcia lub zwrotu danych.

ZAŁĄCZNIK I do umowy powierzenia przetwarzania danych osobowych
numer…….
Z dnia……

Wykaz stron

Administrator (administratorzy): [dane identyfikacyjne i kontaktowe administratora (administratorów) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez administratora]

a) Imię i nazwisko lub nazwa:
……
…… ……
……..
b) Adres:
……
…… ……
……
c) Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:
……
……
d) Imię i nazwisko, Inspektora Ochrony Danych i dane kontaktowe (jeśli powołano):
……

Podpis i data przystąpienia:
……

Podmiot przetwarzający (podmioty przetwarzające): [dane identyfikacyjne i kontaktowe podmiotu przetwarzającego (podmiotów przetwarzających) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez podmiot przetwarzający]

a) Imię i nazwisko lub nazwa:
……..
……..
b) Adres:
……..
……..
……..
c) Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:
……...
d) Imię i nazwisko, Inspektora Ochrony Danych i dane kontaktowe (jeśli powołano):
……

Podpis i data przystąpienia:
……

ZAŁĄCZNIK II do umowy powierzenia przetwarzania danych osobowych
numer…….
Z dnia……

Opis przetwarzania

Kategorie osób, których dane osobowe są przetwarzane

.....

Kategorie przetwarzanych danych osobowych

Zwykłe dane osobowe uczestników:

- imię i nazwisko,
- podpis,
- dane dotyczące wykształcenia,
- numer prawa wykonywania zawodu.

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa.

.....

Charakter przetwarzania

Przetwarzanie danych następuje w formie papierowej lub w systemie informatycznym. Obejmuje następujące czynności przetwarzania: zbieranie, utrwalanie, przechowywanie, wykorzystywanie, archiwizowanie, usuwanie.

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

Dane osobowe przetwarzane są w celu realizacji umowy – .....
.....

Czas trwania przetwarzania

Okres przetwarzania obejmuje czas niezbędny do realizacji przedmiotu umowy głównej.

W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania.

ZAŁĄCZNIK III do umowy powierzenia przetwarzania danych osobowych
numer…….
z dnia……

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych

UWAGA WYJAŚNIAJĄCA:
Środki techniczne i organizacyjne ***należy opisać szczegółowo, a nie w sposób ogólny****.*

Przykłady możliwych środków (uzupełnia podmiot przetwarzający), w przypadku brak zastosowania środka pozostawia się puste pole lub wpisuje nie dotyczy:

1. **Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych**

   Nie dotyczy.

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

   Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie do przetwarzania danych, prowadzona jest ich ewidencja. Dostęp do systemów operacyjnych komputerów zabezpieczony jest poprzez uwierzytelnienie. System wymusza zmianę hasła co 30 dni.

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

   Tworzone są kopie zapasowe danych osobowych.

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

   Zbierane są informacje na temat incydentów, zdarzeń. Stosowane są firewalle i programy antywirusowe, systemy zarządzania kontrolą dostępu.

5. **Środki umożliwiające identyfikację i autoryzację użytkowników**

   Użytkownicy logują się do systemów za pomocą loginu i hasła.

6. **Środki zapewniające ochronę danych w czasie ich przekazywania**

   Przekazywane dane zabezpieczone są hasłem, które odbiorca otrzymuje inną drogą.

7. **Środki zapewniające ochronę danych w czasie ich przechowywania**

   Dane w formie papierowej przechowywane są w szafkach zamykanych na klucz. Na komputerach zainstalowane zostały systemy antywirusowe. Do przechowywania danych wykorzystywane są wyłącznie służbowe nośniki.

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

   W pomieszczeniach, w których przetwarzane są dane, zastosowano np. drzwi antywłamaniowe, system alarmowy, czujniki ruchu, rolety antywłamaniowe. Dostęp do pomieszczenia całodobowo nadzorowany jest przez pracowników firmy świadczącej usługę ochrony osób i mienia. Dane przechowywane są w szafkach zamykanych na klucz.

9. **Środki umożliwiające rejestrowanie zdarzeń**

   Analiza logów IPS na firewallu.

10. **Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej**

    Nie dotyczy.

11. **Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT**
    W SUM wdrożono Zarządzenie Rektora SUM z dnia 17.07.2020 r. nr 129/2020 w sprawie: Systemu Zarządzania Bezpieczeństwem Informacji i ochrony danych osobowych przetwarzanych w Śląskim Uniwersytecie Medycznym w Katowicach:
    Instrukcja Bezpieczeństwa dla Użytkownika Systemów Informatycznych w Śląskim Uniwersytecie Medycznym w Katowicach,
    Instrukcja Bezpieczeństwa w zakresie Zarządzania Systemami Informatycznymi w Śląskim Uniwersytecie Medycznym w Katowicach,
    Instrukcja Bezpieczeństwa w zakresie Klasyfikacji Informacji,
    Instrukcja Bezpieczeństwa w zakresie Zarządzania Ciągłością Działania Śląskiego Uniwersytetu Medycznego w Katowicach

12. **Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów**

    Nie dotyczy.

13. **Środki zapewniające minimalizację danych**

    Przetwarzane są tylko takie dane osobowe, które konieczne są do realizacji usługi.

14. **Środki zapewniające odpowiednią jakość danych**

    Nie dotyczy.

15. **Środki zapewniające ograniczone zatrzymywanie danych**

    Nie dotyczy.

16. **Środki zapewniające rozliczalność**

    Dane osobowe zabezpiecza się przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu.

17. **Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania**

    Nie dotyczy.

W przypadku przekazywania danych podmiotom przetwarzającym lub podprzetwarzającym należy również opisać konkretne środki techniczne i organizacyjne, jakie powinien zastosować podmiot przetwarzający lub podprzetwarzający, aby móc udzielić pomocy administratorowi.

……..
……..
……..
……..
……..
……..

§1

Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy administratorowi: 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. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze podmiot przetwarzający wdrażaja odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
3. 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.

4. 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.
5. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych Podmiot przetwarzający ustanowi dodatkowe.

ZAŁĄCZNIK IV do umowy powierzenia przetwarzania danych osobowych
numer…….
Z dnia……

Wykaz podmiotów podprzetwarzających

UWAGA WYJAŚNIAJĄCA:
Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających (klauzula 7.7 lit. a), opcja 1).

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. Imię i nazwisko lub nazwa:
   ……
   1.1. Adres: ……
   1.2. Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:
   ……
   ……
   ……
   ……
   1.3. Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):
   ……
   ……
   ……
   ……

(należy dopisać odpowiednio kolejne jeśli ma to zastosowanie)

……
Data i podpis Administratora Danych