Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy: (zwana dalej „Umową")

Sieć Badawcza Łukasiewicz – Krakowskim Instytutem Technologicznym, ul. Zakopiańska 73, 30-418 Kraków, wpisanym do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000861401, NIP: 6750000088, REGON: 387116932, zwany w dalszej części umowy **„Podmiotem przetwarzającym"**, reprezentowanym przez:
dr hab. inż. Damiana Gąsiorka, prof. PŚ

a

_____

zwany w dalszej części umowy **„Administratorem"**
reprezentowana przez:

_____

zwanymi dalej łącznie lub z osobna **Stronami**,

zawarta w związku z realizacją umowy z dnia _____ [1]r. zawartej pomiędzy Stronami, zwanej dalej **Umową główną**.

§ 1

1. Administrator oświadcza, że jest Administratorem w rozumieniu art. 4 pkt 7 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 (ogólnego rozporządzenia o ochronie danych, zwanego dalej RODO) w stosunku do danych osobowych powierzonych Podmiotowi Przetwarzającemu.
2. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
3. Podmiot Przetwarzający oświadcza, że jest podmiotem przetwarzającym w rozumieniu art. 4 pkt 8 RODO.
4. Podmiot Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową powierzenia, RODO oraz z innymi przepisami powszechnie obowiązującego prawa.
5. Podmiot Przetwarzający ponosi odpowiedzialność za przetwarzanie powierzonych danych osobowych niezgodnie z Umową powierzenia, RODO lub z innymi przepisami powszechnie obowiązującego prawa, a w szczególności za przypadkowe lub niezgodne z prawem zniszczenie, utratę, modyfikację, nieuprawnione ujawnienie lub dopuszczenie do nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w ramach realizacji Umowy głównej.
6. Jeśli w niniejszej umowie użyto terminów zdefiniowanych w rozporządzeniu (UE) 2016/679, terminy te mają takie same znaczenie jak w RODO.

[1] Należy wprowadzić datę zawarcia Umowy głównej, w związku z którą zawierana jest Umowa powierzenia

7. W razie sprzeczności między zapisami niniejszej umowy a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszej umowy lub zawartych po jej uzgodnieniu, pierwszeństwo mają zapisy poniższej umowy.

§2
Przedmiot i czas trwania przetwarzania

1. Administrator powierza Podmiotowi Przetwarzającemu czynności przetwarzania danych osobowych, dokonywane w jego imieniu.
2. Przedmiot powierzonych czynności przetwarzania danych osobowych stanowi świadczenie usług kontrolingu finansowego na rzecz Administratora wykonywane w ramach realizacji Umowy głównej.

3. Powierzenie czynności przetwarzania następuje na czas:

   x oznaczony, wynoszący 12 miesięcy,
   □ nieoznaczony.
4. Niezależnie od czasu powierzenia czynności przetwarzania danych osobowych, wypowiedzenie lub wygaśnięcie Umowy powierzenia lub Umowy głównej skutkuje zakończeniem czasu powierzenia czynności przetwarzania, o którym stanowi pkt 3.

§ 3
Charakter i cel przetwarzania

1) 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 poprzez[2]:
   a) korespondencję e-mail oraz zapisy w systemach obiegowych Administratora
   b) ……..
2) Sposób dokonywania przez Podmiot Przetwarzający czynności przetwarzania danych osobowych powierzonych przez Administratora obejmuje ich przechowywanie oraz:

   x odczyt / dostęp,
   x edycję,
   x analizę,
   x archiwizację,
   x usuwanie.

3) Czynności przetwarzania danych osobowych są wykonywane w imieniu Administratora w sposób:

   □ jednorazowy,
   x ciągły.

4) Czynności przetwarzania danych osobowych są wykonywane w imieniu Administratora w odniesieniu do:

[2] Wskazać sposoby i kanały dokumentowania poleceń pomiędzy stronami.

□ pojedynczych powierzonych danych,
x całości powierzonych danych.

5) Celem przetwarzania danych osobowych jest realizacja i wsparcie usługi kontrolingu finansowego, w tym przygotowywanie planów i raportów, analiz finansowo-operacyjnych, doradztwa oraz monitoringu realizacji planów i prognoz.
5. Podmiot przetwarzający przetwarza powierzone dane osobowe tylko w zakresie celu/celów wskazanych w niniejszej umowie, chyba że otrzyma dalsze polecenia od Administratora

§ 4
Rodzaj danych i kategorie osób, których dane dotyczą

1. Administrator powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych:

   a. Kategorie osób: pracownicy Administratora, członkowie zespołów projektowych, współpracownicy/wykonawcy, osoby kontaktowe po stronie kontrahentów,
   b. _____.

2. Zakres kategorii danych osobowych powierzonych Podmiotowi Przetwarzającemu obejmuje:
   a. Kategorie danych: identyfikacyjne (imię, nazwisko, stanowisko), kontaktowe (e-mail, telefon), dane projektowe i organizacyjne (przynależność do zespołów), dane finansowe związane z realizacją projektów i budżetów – w zakresie niezbędnym do realizacji usługi,
   b. _____.

§5
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. Szczegółowy wykaz oraz opis środków technicznych i organizacyjnych stosowanych przez Podmiot Przetwarzający, obejmujących elementy wskazane w art. 32 RODO, został przedstawiony w Załączniku nr 1 – „Lista sprawdzająca środków bezpieczeństwa Podmiotu Przetwarzającego", który stanowi integralną część niniejszej Umowy.
3. Administrator oświadcza, że przed zawarciem niniejszej Umowy:
   a) otrzymał od Podmiotu Przetwarzającego informacje dotyczące organizacji procesów przetwarzania danych osobowych, stosowanych środków ochrony oraz poziomu bezpieczeństwa przetwarzania danych,
   b) zapoznał się z tymi informacjami, zweryfikował je z należytą starannością oraz uznał je za zapewniające spełnienie wymogów art. 28 i 32 RODO,
   c) akceptuje opisane w Załączniku nr 1 środki techniczne i organizacyjne jako adekwatne i odpowiednie do powierzenia przetwarzania danych osobowych zgodnie z Umową.
4. Podmiot Przetwarzający potwierdza, że środki przedstawione w Załączniku nr 1 zostały przez niego wdrożone oraz są utrzymywane przez cały okres obowiązywania Umowy. Wszelkie zmiany tych środków, które mogłyby prowadzić do obniżenia poziomu bezpieczeństwa, wymagają uprzedniego pisemnego poinformowania Administratora i jego akceptacji.

5. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
6. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
8. Podmiot przetwarzający bezzwłocznie powiadamia Administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez Administratora narusza rozporządzenie (UE) 2016/679 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.
9. 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.
10. 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 powyższe obowiązki, Podmiot przetwarzający stosuje się do poleceń Administratora.
11. Podmiot przetwarzający pomaga Administratorowi w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
    a. 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;
    b. obowiązek skonsultowania się z właściwym organem nadzorczym przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu jego ograniczenia;
    c. 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;
    d. obowiązki określone w] art. 32 rozporządzenia (UE) 2016/679.
12. Strony określają odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać Administratorowi w stosowaniu przepisów dotyczących ochrony danych osobowych, jak również zakres wymaganej pomocy:

a. Zapewnienie wsparcia w realizacji praw osób, których dane dotyczą, w szczególności poprzez niezwłoczne przekazywanie Administratorowi wszelkich wniosków lub żądań otrzymanych przez Podmiot Przetwarzający, za pośrednictwem ustalonych kanałów komunikacji (w tym służbowej poczty elektronicznej, Microsoft Teams lub innego zatwierdzonego kanału elektronicznego), oraz wykonywanie poleceń Administratora dotyczących obsługi tych żądań przez wyznaczoną osobę odpowiedzialną po stronie Podmiotu Przetwarzającego.
b. Udzielanie Administratorowi niezbędnej pomocy w zapewnieniu zgodności z obowiązkami wynikającymi z art. 32–36 RODO, w szczególności poprzez przekazywanie informacji, wyjaśnień i dokumentacji wymaganej do oceny ryzyka, oceny skutków (DPIA), konsultacji z organem nadzorczym, obsługi incydentów oraz zgłaszania naruszeń, za pośrednictwem uzgodnionych kanałów komunikacji i przez osobę wyznaczoną przez Podmiot Przetwarzający do kontaktu w sprawach ochrony danych osobowych.

§6
Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 5 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. Administrator może przeprowadzić kontrolę samodzielnie lub upoważnić do jego przeprowadzenia niezależnego kontrolera. Kontrole mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Kontrole te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
6. Na wniosek właściwego organu nadzorczego strony są zobowiązane do udostępnienia mu informacji dotyczących wyników przeprowadzonych kontroli.

§7
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom (podmioty podpowierzające) jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający ma obowiązek złożyć w formie pisemnej (na 14 dni przed rozpoczęciem korzystania z usług podmiotu podpowierzajacego) wniosek do Administratora wraz z informacjami niezbędnymi do tego, by Administrator mógł podjąć decyzję w sprawie zgody.
3. Strony są zobowiązane do aktualizacji wykazu podmiotów podopowierzających bez zbędnej zwłoki.
4. 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

5. 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. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
6. Jeśli 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.
7. Podwykonawca, o którym mowa w §7 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
8. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
9. W sytuacji gdy podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub staje się niewypłacalny umowa podpowierzenia przestaje obowiązywać i podmiot podpowierzający ma obowiązek usunięcia.

§ 8
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 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.
3. 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.

§9
Zgłaszanie naruszenia ochrony danych osobowych

1. 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, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.
2. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Administratora podmiot przetwarzający wspomaga Administratora:
   a. przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu 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:
      - 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;
      - możliwe konsekwencje naruszenia ochrony danych osobowych;
      - 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.
3. 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, nie później niż w ciągu 24 godzin. 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.
4. 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.

§10
Rozwiązanie umowy

1. Administrator 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;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora;
d) nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego organu nadzorczego dotyczącej jego obowiązków wynikających z niniejszej umowy lub rozporządzenia (UE) 2016/679;

2. Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszą umową, jeżeli po zawiadomieniu Administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne a Administrator nalega na wypełnienie polecenia.
3. 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.
4. Każda ze stron może rozwiązać umowę za z zachowaniem 30-dniowego okresu wypowiedzenia.
5. Rozwiązanie niniejszej umowy oraz nie zawarcie niezwłocznie kolejnej powoduje rozwiązanie Umowy głównej.

§11
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy otrzymanych danych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§12
Wykaz stron

3. Administrator [*dane identyfikacyjne i kontaktowe Administratora oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez Administratora*]

- Imię i nazwisko lub nazwa: .....

  Adres: .....

- Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

  .....

- Imię, nazwisko i dane kontaktowe inspektora ochrony danych:

  .....

4. Podmiot przetwarzający [*dane identyfikacyjne i kontaktowe podmiotu przetwarzającego oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez podmiot przetwarzający*]

- Imię i nazwisko lub nazwa: .....

  Adres: .....

- Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

  .....

- Imię, nazwisko i dane kontaktowe inspektora ochrony danych:

  .....

§14

Postanowienia końcowe

1. Umowa została sporządzona *w dwóch jednobrzmiących egzemplarzach dla każdej ze stron/w postaci elektronicznej opatrzonej podpisami kwalifikowanymi* (stosuje się odpowiednio)
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora.

Załączniki:
1.Lista sprawdzająca środków bezpieczeństwa Podmiotu przetwarzającego (RODO)

_____ _____

Administrator Podmiot przetwarzający

Załącznik nr 1 do umowy

Lista sprawdzająca Podmiotu przetwarzającego (RODO)

Lp.	Kryterium	TAK	NIE
1. Dane identyfikacyjne podmiotu przetwarzającego			
1.1	Podmiot podał pełne dane identyfikacyjne (nazwa, adres, NIP/KRS/REGON).	☐	☐
1.2	Podmiot wskazał osobę odpowiedzialną za ochronę danych.	☐	☐
1.3	Podmiot powołał Inspektora Ochrony Danych (jeżeli dotyczy).	☐	☐
2. Zgodność z RODO i obowiązkami art. 28			
2.1	Podmiot przetwarzający zna i stosuje obowiązki wynikające z art. 28 RODO.	☐	☐
2.2	Przetwarza dane wyłącznie na polecenie administratora.	☐	☐
2.3	Pracownicy mają podpisane zobowiązania do zachowania poufności.	☐	☐
2.4	Osoby przetwarzające dane zostały odpowiednio przeszkolone.	☐	☐
3. Środki techniczne i organizacyjne– art. 32 RODO			
3.1	Stosowane jest silne uwierzytelnianie (np. 2FA).	☐	☐
3.2	Nadawanie uprawnień odbywa się zgodnie z zasadą need-to-know.	☐	☐
3.3	Regularnie weryfikuje się uprawnienia użytkowników.	☐	☐
Bezpieczeństwo IT			
3.4	Dane są szyfrowane w spoczynku.	☐	☐
3.5	Dane są szyfrowane w transmisji (TLS 1.2+).	☐	☐
3.6	Stosowane są mechanizmy firewall i IDS/IPS.	☐	☐
3.7	Systemy są regularnie aktualizowane i instalowane łaty bezpieczeństwa.	☐	☐
3.8	Funkcjonują kopie zapasowe danych.	☐	☐
3.9	Testuje się proces przywracania danych.	☐	☐
Organizacja i polityki			

3.10	Podmiot posiada formalne polityki bezpieczeństwa.	☐	☐
3.11	Stosowana jest polityka czystego biurka i ekranu.	☐	☐
3.12	Prowadzony jest rejestr incydentów bezpieczeństwa.	☐	☐
Ciągłość działania			
3.13	Podmiot posiada procedury BCP (Plan Ciągłości Działania).	☐	☐
3.14	Podmiot posiada procedury DRP(plan odzyskania po katastrofie).	☐	☐
4. Podwykonawcy (subprocesorzy)			
4.1	Podmiot nie korzysta z podwykonawców bez zgody administratora.	☐	☐
4.2	Przedstawiono listę planowanych podwykonawców (jeśli dotyczy).	☐	☐
4.3	Umowy z podwykonawcami spełniają wymogi art. 28 RODO.	☐	☐
4.4	Subprocesorzy zapewniają równoważny poziom bezpieczeństwa.	☐	☐
5. Zgłaszanie incydentów			
5.1	Podmiot posiada procedurę zgłaszania incydentów.	☐	☐
5.2	Zobowiązuje się zgłaszać incydenty administratorowi niezwłocznie (max 24h).	☐	☐
5.3	Prowadzi rejestr naruszeń.	☐	☐
6. Transfery danych do państw trzecich			
6.1	Dane są przetwarzane wyłącznie na terenie EOG.	☐	☐
6.2	(Jeśli NIE) wskazano kraje transferu.	☐	☐
6.3	Stosowane są standardowe klauzule umowne (SCC 2021).	☐	☐
6.4	Wykonano ocenę TIA (ocean skutków transferu Danych) dla transferów.	☐	☐
7. Lokalizacja przetwarzania			
7.1	Podmiot przedstawił lokalizację serwerów i centrów danych.	☐	☐

7.2	Zobowiązuje się informować administratora o zmianach lokalizacji.	☐	☐
8. Zwrot i usuwanie danych po zakończeniu świadczenia			
8.1	Podmiot zobowiązuje się zwrócić wszystkie dane po zakończeniu umowy.	☐	☐
8.2	Podmiot zobowiązuje się trwale usunąć dane po zakończeniu umowy.	☐	☐
8.3	Zniszczenie danych zostanie potwierdzone protokołem.	☐	☐
9. Audyt i nadzór administratora			
9.1	Podmiot akceptuje możliwość przeprowadzenia audytu.	☐	☐
9.2	Udostępni dokumentację niezbędną do weryfikacji.	☐	☐
9.3	Zapewni współpracę podczas audytu.	☐	☐
10. Dokumentacja i certyfikacje			
10.1	Podmiot posiada aktualną dokumentację bezpieczeństwa.	☐	☐
10.2	Podmiot posiada certyfikat ISO 27001 (jeśli dotyczy).	☐	☐
10.3	Podmiot posiada certyfikat ISO 27701 (jeśli dotyczy).	☐	☐
10.4	Przedstawiono raporty z audytów lub testów bezpieczeństwa.	☐	☐
11. Oświadczenia końcowe			
11.1	Podmiot przestrzega RODO i SCC 2021 (standardowych klauzul umownych).	☐	☐
11.2	Zapewnia środki bezpieczeństwa zgodne z art. 32 RODO.	☐	☐
11.3	Potwierdza prawdziwość udzielonych informacji.	☐	☐