Załącznik nr 1
do Zarządzenia Rektora
nr R.0211.34.2022 z dnia 4 lipca 2022 roku

POLITYKA BEZPIECZEŃSTWA
w zakresie ochrony danych osobowych
w Uniwersytecie Ekonomicznym w Krakowie

W ramach realizacji celów statutowych oraz innych celów wynikających z przepisów prawa Uniwersytet Ekonomiczny w Krakowie (dalej „Uczelnia" lub „UEK"), jako administrator danych osobowych stosuje politykę bezpieczeństwa w zakresie danych osobowych i spełnia wymagane prawem obowiązki wobec osób, których dane dotyczą.
Mając powyższe na uwadze ustala się następujące wytyczne polityki bezpieczeństwa danych osobowych w Uczelni, zwane dalej „Polityką bezpieczeństwa":

Rozdział I.
Postanowienia ogólne

§ 1

Przetwarzanie danych osobowych w Uczelni jest dopuszczalne pod warunkiem przestrzegania przepisów:

1) 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 praz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) – dalej RODO;
2) przepisów innych ustaw, a także rozporządzeń normujących problematykę przetwarzania danych osobowych;
3) wewnętrznych aktów normatywnych Uczelni (uchwał Senatu UEK i zarządzeń Rektora) regulujących sprawy dotyczące ochrony danych osobowych.

§ 2

Uczelnia przetwarza dane osobowe:

1) w związku z realizacją zadań uczelni, wynikających z Ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (t. j. Dz. U. z 2022 r., poz. 574, z późn. zm.),
2) w celu zapewnienia prawidłowej, zgodnej z prawem polityki personalnej oraz wypełnienia obowiązków prawnych ciążących na administratorze, jako pracodawcy,
3) dla realizacji innych celów i zadań – w szczególności wynikających z przepisów prawa lub prawnie uzasadnionych interesów administratora,
4) w pozostałych, prawnie uzasadnionych celach – za zgodą osób, których dane dotyczą.

§ 3

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych, uwzględniając zasady wynikające z art. 5 RODO zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości);

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami (zasada ograniczenia celu, celowości);
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą (zasada ograniczenia przechowywania);
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności);
7) przetwarzane w sposób, który pozwoli administratorowi wykazać, iż spełnione są zasady wymienione w pkt 1-6 (zasada rozliczalności).

2. Szczególnej ochronie podlegają dane osobowe wymienione w art. 9 ust. 1 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, a także dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa – art. 10 RODO.

§ 4

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych odnosi się do danych osobowych przetwarzanych w:
   1) zbiorach danych tradycyjnych, na papierowych nośnikach danych (dokumentacja papierowa, np. kartoteki, księgi, wykazy, listy itp.),
   2) systemach informatycznych i na nośnikach cyfrowych,
   3) systemach dozoru wizyjnego (monitoring).
2. Polityka bezpieczeństwa w zakresie ochrony danych osobowych realizowana jest w Uniwersytecie Ekonomicznym w Krakowie przez wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, w szczególności przez osoby odpowiedzialne za nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z przepisów prawa oraz uregulowań wewnętrznych w tym zakresie, tj.:
   1) administratora danych osobowych (w osobie rektora) – **ADO** – zgodnie art. 24 RODO
   2) inspektora ochrony danych – **IOD** – zgodnie z art. 39 RODO
   3) inne osoby wykonujące zadania dotyczące przetwarzania i ochrony danych osobowych na podstawie udzielonych im upoważnień, w szczególności administratora/-ów systemów informatycznych - **ASI**.
3. Polityka bezpieczeństwa obowiązuje we wszystkich obiektach, lokalizacjach, komórkach organizacyjnych i stanowiskach pracowniczych Uczelni. Odnosi się do wszystkich

chronionych danych osobowych przetwarzanych w Uczelni, niezależnie od formy, celu oraz zakresu ich przetwarzania (tradycyjnego i elektronicznego).

4. Procedury i zasady określone w Polityce bezpieczeństwa mają zastosowanie do wszystkich osób wykonujących prace związane z działalnością Uczelni lub na rzecz Uczelni (niezależnie od formy współpracy, czy rodzaju umowy) w szczególności pracowników, współpracowników (w tym zleceniobiorców i osób realizujących umowy o dzieło) oraz innych osób, którym zostało udzielone upoważnienie do przetwarzania danych osobowych.
5. UEK, jego pracownicy i współpracownicy deklarują pełne zaangażowanie dla bezpieczeństwa przetwarzania danych osobowych przetwarzanych zarówno w sposób tradycyjny, jak i w systemach informatycznych oraz na nośnikach cyfrowych.

§ 5

Uczelnia, jako administrator danych stosuje środki organizacyjne i techniczne, w tym informatyczne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, w szczególności wprowadza rozwiązania dotyczące:

1) pseudonimizacji i szyfrowania danych osobowych,
2) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych,
3) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, skutkującego naruszeniem ochrony danych osobowych,
4) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§ 6

Dokumentacja dotycząca sposobu przetwarzania danych oraz środki ochrony danych osobowych powstają w oparciu o:

1) przepisy prawa powszechnie obowiązującego,
2) niniejszą Politykę bezpieczeństwa w zakresie ochrony danych osobowych,
3) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) inne wewnętrzne akty normatywne Uczelni, w tym zarządzenia Rektora, a także instrukcje, wytyczne i polecenia służbowe określające zasady i procedury dotyczące ochrony danych osobowych, wydawane przez upoważnione do tego osoby w poszczególnych jednostkach organizacyjnych.

Rozdział II.
Zasady udostępniania danych osobowych oraz prawa osób, których dane osobowe są przetwarzane w Uczelni

§ 7

1. Uczelnia, jako administrator danych udostępnia przetwarzane w swoich zasobach dane osobowe wyłącznie:

    1) osobom, które przetwarzają dane osobowe na polecenie administratora tj. posiadającym upoważnienie do przetwarzania danych osobowych – co do zbioru i zakresu. Wzór upoważnienia stanowi Załącznik nr 1 do niniejszej Polityki. Upoważnienia są wydawane przez ADO po wcześniejszej akceptacji IOD.

Upoważnienie może być cofnięte przed upływem okresu, na jaki zostało wydane – wzór cofnięcia upoważnienia stanowi Załącznik nr 2. Wszystkie osoby, którym zostaje udzielone upoważnienie do przetwarzania danych osobowych są zobowiązane do podpisania oświadczenia o zachowaniu poufności danych osobowych – wzór oświadczenia stanowi Załącznik nr 3 do niniejszej Polityki.

2) podmiotom przetwarzającym, tj. osobom lub podmiotom, których charakter pracy wymaga udostępnienia im takich danych – na podstawie umowy powierzenia przetwarzania danych osobowych, która w szczególności określa:
   a) przedmiot i czas trwania przetwarzania
   b) charakter i cel przetwarzania
   c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą
   d) obowiązki podmiotu przetwarzającego wynikające z art. 28 RODO

   Wzór umowy powierzenia przetwarzania danych osobowych stosowany w Uczelni stanowi Załącznik nr 4 do niniejszej Polityki.
3) podmiotom kontrolnym uprawnionym do kontroli działalności administratora oraz podmiotom uprawnionym do przetwarzania danych osobowych – na podstawie przepisów prawa.

2. Dostęp do danych osobowych, o którym mowa w ust. 1 pkt 3, po okazaniu dokumentów potwierdzających uprawnienia mogą mieć w szczególności pracownicy: Państwowej Inspekcji Pracy, Zakładu Ubezpieczeń Społecznych, organów kontroli skarbowej, Policji i służb specjalnych (Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego), sądów powszechnych, Najwyższej Izby Kontroli, Urzędu Ochrony Danych Osobowych, a także inne osoby, podmioty i organy upoważnione przez przepisy prawa i działające w granicach przyznanych im uprawnień.

§ 8

1. Osoba, której dane osobowe dotyczą, na podstawie art. 15 RODO ma prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane w Uczelni, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji o:
   1) celu przetwarzania;
   2) kategorii odnośnych danych osobowych;
   3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   4) w miarę możliwości - planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
   5) prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz prawie do wniesienia sprzeciwu wobec takiego przetwarzania;
   6) prawie wniesienia skargi do organu nadzorczego;
   7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
   8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Uczelnia, jako administrator danych, w ramach wypełnienia tzw. obowiązku informacyjnego określonego w art. 13 i 14 RODO podaje informacje wskazane w ust.1 w stosownych klauzulach informacyjnych przygotowywanych pod nadzorem IOD. Klauzule informacyjne są zamieszczane na stronach internetowych Uczelni, stanowią załączniki

w poczcie elektronicznej lub są przekazywane odpowiednim adresatom wraz z dokumentacją papierową.

3. W przypadkach i na zasadach określonych w art. 16-22 RODO, osoba, której dane osobowe dotyczą ma prawo do:
    1) żądania, aby jej dane osobowe zostały niezwłocznie sprostowane, jeżeli są nieprawidłowe lub aby zostały uzupełnione, jeżeli dane te są niekompletne,
    2) żądania usunięcia danych osobowych,
    3) żądania ograniczenia przetwarzania danych osobowych,
    4) otrzymania w określonym formacie danych osobowych i przesłania ich do innego administratora lub żądania przesłania takich danych bezpośrednio innemu administratorowi,
    5) wniesienia sprzeciwu – z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania jej danych osobowych,
    6) niepodlegania decyzji podjętej wyłącznie na podstawie przetwarzania, które odbywa się w sposób zautomatyzowany (np. profilowanie)

Rozdział III.
Obszary przetwarzania danych osobowych oraz zastosowane w nich środki techniczne i organizacyjne zapewniające przetwarzanie danych zgodnie z RODO

§ 9

1. Za fizyczny obszar przetwarzania danych osobowych w Uczelni uważa się wszystkie budynki, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe na nośnikach papierowych. W szczególności jest to obszar bieżącego przechowywania dokumentów oraz obsługi osób, których dane dotyczą.
2. Za wirtualny obszar przetwarzania danych osobowych w Uczelni uważa się miejsce, w którym znajduje się urządzenie umożliwiające dostęp do danych osobowych przetwarzanych w systemie informatycznym. Za szczególny wirtualny obszar przetwarzania danych osobowych uważa się tzw. chmurę, czyli usługę internetową umożliwiającą tworzenie, udostępnianie, przesyłanie i przechowywanie plików (dokumentów, zdjęć, plików multimedialnych itp.) oraz komunikowanie się i pracę grupową w formie online, z użyciem serwerów niebędących własnością Uczelni, których wydzielona część udostępniona jest w ramach wykupionej licencji (np. wirtualny dysk OneDrive, usługa SharePoint, przestrzeń dyskowa przydzielana dla zespołów w Microsoft Teams).

§ 10

1. W obszarze fizycznym przetwarzania danych osobowych w Uczelni zastosowane są rozwiązania uniemożliwiające dostęp osób nieuprawnionych oraz zapobiegające wystąpieniu przypadkowych zdarzeń o charakterze siły wyższej. W szczególności są to zabezpieczenia fizyczne, takie jak:
    1) wzmocnione drzwi,
    2) pomieszczenia zamykane na klucz,
    3) wejścia kodowane,
    4) elektroniczne systemy alarmowe,
    5) zamykane na klucz meble biurowe,
    6) zabezpieczenie okien (kraty i folia antywłamaniowa),
    7) dostęp z użyciem kart elektronicznych i systemów jednoznacznie rejestrujących fakt użycia takiej karty,
    8) alarm przeciwpożarowy,
    9) system dozoru wizyjnego z użyciem kamer,
    10) alarm antywłamaniowy.

2. Jeżeli dane osobowe przetwarzane są tylko w części pomieszczenia, pomieszczenie takie w miarę możliwości powinno być wyraźnie podzielone na:
    1) część ogólnodostępną,
    2) część, w której przetwarzane są dane osobowe.
3. Wydzielenie części pomieszczenia może być w szczególności dokonane poprzez:
    1) montaż barierek lub lad,
    2) odpowiednie ustawienie mebli biurowych.
4. W obszarze fizycznym przetwarzania danych osobowych mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych.
5. Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w obszarze fizycznym przetwarzania danych osobowych wyłącznie w obecności upoważnionego pracownika.
6. Dostęp do budynków i pomieszczeń, w których przetwarzane są dane osobowe podlega nadzorowi i kontroli.
7. Nadzór, o którym mowa w ust. 6 dokonywany jest w danej jednostce organizacyjnej przez jej kierownika. Kierownik jednostki organizacyjnej, w której przetwarzane są dane osobowe pisemnie informuje portiera wydającego klucze o osobach upoważnionych do wejścia do pomieszczeń, w których przetwarzane są dane osobowe. Klucze mogą być wydawane wyłącznie pracownikom upoważnionym przez ADO do przetwarzania danych osobowych lub innym osobom uprawnionym do dostępu do fizycznego obszaru przetwarzania danych osobowych w Uczelni.
8. Kontrola, o której mowa w ust. 6 polega na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. Czynność tę wykonują osoby pracujące w portierniach. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz datę i godzinę pobrania lub zwrotu klucza.
9. Szczególne zasady udzielania dostępu do wybranych, specyficznych obiektów fizycznego obszaru przetwarzania danych osobowych w Uczelni określane są przez osoby kierujące poszczególnymi jednostkami organizacyjnymi Uczelni, w których takie obiekty występują. W przypadku nie określenia szczegółowych zasad stosuje się przepisy niniejszej Polityki.

§ 11

1. W obszarze wirtualnym przetwarzania danych osobowych w Uczelni zastosowane są rozwiązania uniemożliwiające dostęp osób nieuprawnionych oraz zapobiegające wystąpieniu przypadkowych zdarzeń o charakterze siły wyższej. W szczególności są to zabezpieczenia techniczne/informatyczne, takie jak:
    1) dostęp do systemu informatycznego poprzez logowanie,
    2) wymóg stosowania haseł o odpowiednio wysokim stopniu skomplikowania,
    3) tworzenie kopii zapasowych baz danych zawierających dane osobowe,
    4) ograniczenie ruchu dla usług publicznych i jego ochrona przy pomocy access-list na routerach i udostępnianie tylko wybranych portów na serwerach,
    5) stosowanie zapory ogniowej (firewall) oraz jej bieżący monitoring,
    6) stosowanie ochrony antywirusowej, antyszpiegowskiej i antyreklamowej,
    7) bieżąca aktualizacja oprogramowania,
    8) weryfikacja podmiotów świadczących usługi hostingu lub dostawców usług SaaS (Software as a Service),
    9) zezwolenie na przetwarzanie danych osobowych stanowiących zasoby Uczelni przy użyciu komputerów przenośnych – wyłącznie w przypadkach, gdy komputery takie stanowią wyposażenie pracowników (sprzęt służbowy) i są odpowiednio zabezpieczone (zaszyfrowane);

10) zezwolenie na przetwarzanie, w szczególności przechowywanie danych osobowych stanowiących zasoby Uczelni na nośnikach cyfrowych (dysk przenośny, pendrive itp.) – wyłącznie w przypadkach, gdy nośniki takie stanowią wyposażenia pracowników (sprzęt służbowy) i są odpowiednio zabezpieczone (zaszyfrowane);
11) zakaz przetwarzania danych osobowych, które nie stanowią zasobów Uczelni (dane prywatne) na służbowym sprzęcie.

2. Pod szczególną ochroną pozostają urządzenia stanowiące zasoby sprzętowe systemu informatycznego – stacje robocze pracowników przetwarzających dane osobowe wchodzące w skład tego systemu powinny być umiejscowione w taki sposób, aby uniemożliwić dostęp osobom nieuprawnionym (w szczególności dostęp do monitorów oraz urządzeń służących do kopiowania danych).

Rozdział VI.
Zasady bezpieczeństwa
zapewniające przetwarzanie danych zgodnie z RODO

§ 12

1. W Uczelni stosowane są następujące zasady bezpiecznego przetwarzania danych osobowych:
   1) zakaz udostępniania haseł dostępu do systemów informatycznych lub pozostawiania ich w łatwo dostępnych miejscach na stanowisku pracy,
   2) zakaz udzielania informacji zawierających dane osobowe w rozmowach przez telefon, z osobami, których tożsamości nie można jednoznacznie zweryfikować i potwierdzić,
   3) wymóg przestrzegania tzw. „polityki czystego biurka” i „polityki czystego pulpitu”,
   4) do codziennej pracy w systemie informatycznym wymóg używania zwykłego konta użytkownika, bez uprawnień administratora,
   5) wymóg zachowania podwyższonej ostrożności wobec wiadomości e-mail otrzymanych od niezweryfikowanych nadawców – zakaz klikania w podejrzane linki i otwierania nieznanych załączników,
   6) wymóg stosowania szyfrowania załączników zawierających dane osobowe, wysyłanych e-mailem poza obszar domeny Uczelni,
   7) wymóg pracy w odpowiednim skupieniu i bez nadmiernego pośpiechu,
   8) podczas opuszczania systemu informatycznego - wymóg wyrobienia nawyku wylogowania poprzez przycisk „Wyloguj/Wyloguj się” zamiast używania krzyżyka w celu zamknięcia okna lub pozostawiania aktywnego dostępu do systemu (bez wylogowania),
   9) po zakończeniu pracy – wymóg bieżącego usuwania zbędnych danych, zarówno w odniesieniu do dokumentów papierowych, jak i w wersji elektronicznej.
2. Podczas pracy w każdym systemie informatycznym stosowane są następujące zasady ogólne:
   1) dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie administratora. Pracownicy/współpracownicy mają dostęp wyłącznie do danych w takim zakresie, jaki został wskazany w upoważnieniu i wynika z umowy o pracę lub umowy cywilnoprawnej oraz przydzielonych zadań/obowiązków (zasada wiedzy koniecznej i zasada minimalizacji danych);
   2) dostęp do systemu jest możliwy wyłącznie po podaniu identyfikatora i właściwego hasła (logowanie). Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, który jest odpowiedzialny za wszystkie czynności wykonywane przy jego użyciu,

3) użytkownik systemu informatycznego jest zobowiązany do logowania się w taki sposób, aby uniemożliwić poznanie loginu i hasła przez osoby nieupoważnione.

§ 13

1. Czasowe (w trakcie pracy) opuszczenie przez pracownika stanowiska, na którym przetwarzane są dane osobowe, wiąże się z zastosowaniem dostępnych środków zabezpieczających, by chronić używane zasoby danych osobowych przed dostępem do nich osób nieuprawnionych.
2. Całkowite (po zakończeniu pracy w danym dniu) opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, wiąże się z zastosowaniem wszystkich dostępnych środków zabezpieczających to pomieszczenie przed wejściem tam osób niepowołanych.
3. Zabronione jest opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zastosowania odpowiedniego zabezpieczenia. Wszelkie konsekwencje takiego naruszenia mogą być traktowane jako niedopełnienie podstawowych obowiązków pracowniczych.

Rozdział V.
Zasady przetwarzania danych osobowych w zbiorach

§ 14

1. Przetwarzane w Uczelni dane osobowe są gromadzone w zbiorach, tworzonych w taki sposób, aby odpowiednie dane były dostępne w oparciu o określone kryteria, niezależnie od tego, czy zestaw danych jest scentralizowany lub zdecentralizowany albo rozproszony funkcjonalnie lub geograficznie.
2. Podstawowymi zbiorami danych tworzonymi w Uczelni są dane osobowe: kandydatów na studia, studentów, doktorantów, uczestników studiów podyplomowych, kursów, szkoleń i innych form kształcenia oferowanych przez UEK (np. Uniwersytet Dziecięcy, Uniwersytet Trzeciego Wieku), absolwentów, uczestników konferencji i wykładów rektorskich, kandydatów do pracy, pracowników, emerytów i członków rodzin pracowników, kontrahentów (w tym zleceniobiorców), interesariuszy, stron oraz innych osób fizycznych, których dane osobowe UEK jest uprawniony przetwarzać na podstawie przepisów prawa lub na podstawie zgody wyrażonej przez osoby, których dane dotyczą.
3. W Uczelni mogą być tworzone również inne zbiory danych, w celach doraźnych, ze względów technicznych lub w związku z realizacją określonego zadania. Zbiory te, po ich wykorzystaniu są niezwłocznie usuwane albo poddane modyfikacji tak, by danych w nich zawartych nie można było przypisać konkretnej lub dającej się ustalić osobie (anonimizacja) lub aby konieczny był w tym celu nieproporcjonalnie duży nakład czasu, kosztów i pracy (pseudonimizacja lub szyfrowanie).
4. Uczelnia sprawuje nadzór nad wszelkimi zbiorami danych osobowych tworzonymi na jej obszarze.
5. Zabronione jest przetwarzanie danych osobowych, w tym tworzenie zbiorów danych, a także gromadzenie w zbiorach lub poza nimi danych osobowych - innych niż niezbędne dla realizacji celów, do których dane te zostały zebrane.
6. Wszelkie nowe programy i systemy informatyczne, które mają służyć gromadzeniu i przetwarzaniu danych osobowych w Uczelni muszą zapewniać możliwość obsługi określonych zbiorów danych oraz spełniać wymogi bezpieczeństwa wskazane przez administratora.

Rozdział VI.
Postanowienia końcowe

§ 15

1. Uczelnia na bieżąco dokłada wszelkich starań, aby gromadzone i przetwarzane dane osobowe podlegały ochronie zgodnie z wymogami obowiązującego w tym zakresie prawa.
2. Mając na uwadze stałe podnoszenie poziomu bezpieczeństwa przetwarzania danych osobowych, Uczelnia na bieżąco wdraża środki techniczne (w tym informatyczne) i organizacyjne, które pozwalają minimalizować ryzyko związane z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Uczelnia wprowadziła akty prawa wewnętrznego regulujące kwestie związane z przetwarzaniem danych osobowych, w szczególności:
    1) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
    2) Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji,
    3) Regulamin użytkowania poczty elektronicznej pracowników UEK,
    4) Regulamin użytkowania studenckiej poczty elektronicznej UEK,
    5) Wzór oświadczenia składanego przez absolwentów UEK dotyczącego przetwarzania danych osobowych przez Uczelnię,
    6) Zasady korzystania ze zbiorów systemu biblioteczno-informacyjnego w UEK,
    7) Zasady postępowania z dokumentami publicznymi funkcjonującymi w UEK,
    8) Zasady zamieszczania rozpraw doktorskich w ramach zasobów cyfrowych Biblioteki Głównej UEK oraz ich udostępniania osobom zainteresowanym,
    9) Zasady przygotowania danych oraz informacji na potrzeby ewaluacji jakości działalności naukowej 2017-2021,
    10) Regulamin użytkowania konta i zasady pracy z wykorzystaniem usług on-line Office 365 w UEK.
4. Uczelnia stosuje środki organizacyjne zapewniające utrzymanie poufności, integralności i rozliczalności przetwarzanych danych osobowych, w szczególności:
    1) prowadzona jest ewidencja osób, którym nadano upoważnienie do przetwarzania danych osobowych;
    2) promowana jest ogólna zasada poufności danych osobowych – w każdym aspekcie funkcjonowania Uczelni;
    3) prowadzone są szkolenia wewnętrzne i wydawane są instrukcje oraz zalecenia podnoszące świadomość pracowników w zakresie bezpieczeństwa przetwarzania danych osobowych;
    4) prowadzona jest ocena ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w związku z przetwarzaniem danych osobowych;
    5) dokonywana jest ocena skutków dla ochrony danych osobowych w odniesieniu do planowanych operacji przetwarzania, w szczególności z użyciem nowych technologii – w przypadku, gdy zostanie stwierdzone, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

§16

1. Niniejsza polityka bezpieczeństwa jest na bieżąco poddawana analizie i w razie potrzeby aktualizowana. IOD analizuje, czy polityka bezpieczeństwa jest adekwatna do zmian:
    a) organizacyjnych w Uczelni, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,

b) w obowiązującym prawie.

2. Wraz z przeglądem Polityki bezpieczeństwa IOD kontroluje również pracowników i inne podmioty upoważnione do przetwarzania danych osobowych pod kątem przestrzegania przez te osoby niniejszej Polityki, Instrukcji zarządzania systemem informatycznym oraz przepisów RODO (audyty doraźne).
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie potwierdzające znajomość jego treści.

Załączniki:

- Zał. 1 – wzór upoważnienia do przetwarzania danych osobowych;
- Zał. 2 – wzór cofnięcia upoważnienia;
- Zał. 3 – wzór oświadczenia o zachowaniu poufności;
- Zał. 4 – wzór umowy powierzenia przetwarzania danych osobowych;

Załącznik nr 1
do Polityki bezpieczeństwa
w zakresie ochrony danych osobowych

Upoważnienie dla osoby przetwarzającej dane osobowe

Działając na podstawie § 7 ust. 1 pkt 1 *Polityki bezpieczeństwa w zakresie ochrony danych osobowych Uniwersytetu Ekonomicznego w Krakowie*

upoważniam Panią/Pana ……..

do przetwarzania danych osobowych, których administratorem jest Uniwersytet Ekonomiczny w Krakowie, **w zbiorach**: ……..

(*tu wpisać nazwy zbiorów, w których upoważniona osoba może przetwarzać dane osobowe, w szczególności należy wybrać spośród: kandydatów na studia, studentów, doktorantów, uczestników studiów podyplomowych, kursów, szkoleń i innych form kształcenia oferowanych przez UEK, absolwentów, uczestników konferencji i wykładów rektorskich, kandydatów do pracy, pracowników, emerytów i członków rodzin pracowników, kontrahentów, interesariuszy, stron oraz innych osób fizycznych, których dane osobowe UEK jest uprawniony przetwarzać na podstawie przepisów prawa lub na podstawie zgody wyrażonej przez osoby, których dane dotyczą*)

na nośnikach papierowych i w wersji elektronicznej, w systemach informatycznych używanych do przetwarzania danych osobowych w Uniwersytecie Ekonomicznym w Krakowie, **w zakresie** niezbędnym do wykonywania obowiązków wynikających z przydzielonego zakresu czynności i poleceń przełożonych w ramach……..

(*tu wpisać, co jest podstawą udzielenia upoważnienia, np. zatrudnienia na stanowisku …….. w ……. (nazwa jednostki organizacyjnej), realizacji umowy nr …….. zawartej dnia ……..*)

Niniejsze upoważnienie jest ważne ……..

(*tu wpisać, do kiedy upoważnienie ma obowiązywać, np. konkretną datę albo przez czas trwania zatrudnienia, do chwili rozwiązania umowy nr …….. z dnia ……...*)

Jednocześnie zastrzegam, że osoby, które zostały upoważnione do przetwarzania danych osobowych w Uniwersytecie Ekonomicznym w Krakowie są obowiązane zachować w poufności przetwarzane dane osobowe oraz sposoby ich zabezpieczenia.

Data wystawienia dokumentu:……

.....
(podpis Rektora)

Powyższe upoważnienie przyjmuję

……
(podpis osoby, której upoważnienie dotyczy)

Cofnięcie upoważnienia dla osoby przetwarzającej dane osobowe

Działając na podstawie § 7 ust. 1 pkt 1 Polityki bezpieczeństwa w zakresie ochrony danych osobowych Uniwersytetu Ekonomicznego w Krakowie

cofam upoważnienie z dnia ……
(data wystawienia upoważnienia)
wystawione dla Pani/Pana ……..

do przetwarzania danych osobowych we wszystkich zbiorach oraz systemach informatycznych, wskazanych w upoważnieniu.

Data wystawienia dokumentu:……..

.....
(podpis Rektora)

Załącznik nr 3
do Polityki bezpieczeństwa
w zakresie ochrony danych osobowych

……
(imię i nazwisko)

……..
(stanowisko)

……..
(jednostka organizacyjna)

Oświadczenie osoby posiadającej dostęp do danych osobowych

Ja niżej podpisana/-y, zobowiązuję się do zachowania poufności danych osobowych, do których przetwarzania zostało mi wydane upoważnienie w związku z wykonywaniem przeze mnie obowiązków w Uniwersytecie Ekonomicznym w Krakowie.

Zobowiązuję się do przestrzegania wszelkich przepisów prawa dotyczących ochrony danych osobowych, w tym wewnętrznych aktów normatywnych Uniwersytetu Ekonomicznego w Krakowie.

Potwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 4 pkt 1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 roku oraz, że zapoznałam/-em się z przepisami dotyczącymi ochrony danych osobowych.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu pracy oraz może być podstawą do realizacji uprawnień przez Uniwersytet Ekonomiczny w Krakowie.

Znam zakres odpowiedzialności karnej określony w Ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych i Ustawie z dnia 6 czerwca 1997 r. Kodeks karny.

……..
(data i podpis osoby składającej oświadczenie)

WZÓR

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
(zwana dalej „Umową")

zawarta dnia _____ w …… pomiędzy:

Uniwersytetem Ekonomicznym w Krakowie siedzibą w Krakowie przy ul. Rakowickiej 27, 30-510 Kraków
zwanym dalej „Administratorem danych" lub „Administratorem"
reprezentowanym przez:
……..
……..
a
……,
zwanym w dalszej części umowy „Podmiotem przetwarzającym" lub „Przetwarzającym"
reprezentowanym przez:
……
……

zwanymi dalej łącznie „Stronami".

Na podstawie art. 28 ust. 3 *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) - zwanego dalej „RODO", a także w związku z *Decyzją Wykonawczą 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 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*, Strony postanawiają, co następuje:

§ 1
POSTANOWIENIA OGÓLNE

1. Przedmiotem niniejszej Umowy jest powierzenie Przetwarzającemu przez Administratora przetwarzania danych osobowych w celu i zakresie wskazanych poniżej.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, odnoszącymi się do ochrony danych osobowych.
3. Podmiot przetwarzający oświadcza, że dysponuje środkami, doświadczeniem, wiedzą i wykwalifikowanym personelem niezbędnymi do przetwarzania danych zgodnie przepisami prawa, o których mowa w ust. 2 powyżej.

4. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
5. Niniejsza Umowa nie odnosi się do zapewnienia przez Strony wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V RODO; w tym zakresie i w razie potrzeby Strony zawrą odrębną umowę.
6. Wszelkie określenia i definicje użyte w niniejszej Umowie odczytuje się i interpretuje zgodnie z przepisami RODO.
7. Niniejsza Umowa nie może być interpretowana w sposób sprzeczny z prawami i obowiązkami wynikającymi z przepisów RODO.
8. W razie sprzeczności między niniejszą Umową a postanowieniami powiązanych umów między Stronami, istniejących w chwili uzgadniania zapisów niniejszej Umowy lub zawartych po ich uzgodnieniu, pierwszeństwo ma niniejsza Umowa.

§ 2
OPIS PRZETWARZANIA POWIERZONYCH DANYCH OSOBOWYCH

1. Administrator powierza Przetwarzającemu przetwarzanie danych osobowych następujących kategorii osób fizycznych: ..... *(należy wymienić określone kategorie np. pracownicy Administratora, studenci, uczestnicy szkolenia itp.)*
2. Administrator powierza Przetwarzającemu przetwarzanie następujących kategorii danych osobowych:
    a. Imię i nazwisko
    b. Adres zamieszkania (kod pocztowy, miasto, ulica, numer domu, numer mieszkania)
    c. Numer telefonu
    d. Adres e-mail
    e. .....
    f. .....

    (należy wymienić pozostałe kategorie danych, jeśli będą przetwarzane)
3. Przetwarzanie danych przez Przetwarzającego będzie miało charakter .....
    *(należy określić czy przetwarzanie będzie **sporadyczne / jednorazowe** czy **systematyczne / ciągłe**)*
4. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu ..... *(należy wskazać konkretny/-e cel-e, w którym/-ch nastąpiło powierzenie danych osobowych, np. realizacja umowy z dnia..... - dalej „Umowa główna")*
5. Przetwarzający będzie przetwarzał powierzone dane osobowe wyłącznie przez czas niezbędny do realizacji celu wskazanego w Umowie głównej i we wskazanym w niej terminie.
6. Powierzenie przetwarzania danych osobowych obejmuje następujące czynności, które może wykonywać Przetwarzający na danych osobowych w związku z realizacją celu, o którym mowa w ust. 4: ..... *(należy wymienić konkretne operacje przetwarzania np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie).*
7. Przetwarzający nie jest uprawniony do dysponowania danymi osobowymi ani decydowania o celach i środkach przetwarzania powierzonych danych osobowych.

§ 3
OBOWIĄZKI PRZETWARZAJĄCEGO

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 Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Za udokumentowane polecenie uznaje się zadania zlecone do wykonywania przez Podmiot przetwarzający zgodnie z Umową główną. Administrator może

wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.

2. Podmiot przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Podmiotu przetwarzającego wydane mu polecenie stanowi naruszenie RODO lub innych przepisów dotyczących ochrony danych osobowych.
3. Podmiot przetwarzający będzie przetwarzał dane wyłącznie w celu wskazanym w § 2 ust. 4, chyba że otrzyma dalsze polecenia od Administratora.
4. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do stosowania co najmniej następujących środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania:
   1) *Posiadanie odpowiednich certyfikatów bezpieczeństwa;*
      ……
   2) *Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych;*
      ……
   3) *Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*
      ……
   4) *Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*
      ……
   5) *Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;*
      ……
   6) *Środki umożliwiające identyfikację i autoryzację użytkowników;*
      ……
   7) *Środki zapewniające ochronę danych w czasie ich przekazywania;*
      ……
   8) *Środki zapewniające ochronę danych w czasie ich przechowywania;*
      ……
   9) *Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe;*
      ……
   10) *Środki umożliwiające rejestrowanie zdarzeń;*
      ……
   11) *Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej;*
      ……
   12) *Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT;*
      ……
   13) *Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów;*
      ……
   14) *Środki zapewniające minimalizację danych;*
      ……
   15) *Środki zapewniające odpowiednią jakość danych;*
      ……
   16) *Środki zapewniające ograniczone zatrzymywanie danych;*
      ……
   17) *Środki zapewniające rozliczalność;*
      ……
   18) *Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania;*

……

(należy wybrać spośród wskazanych powyżej i szczegółowo opisać konkretne środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych)

5. Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania niniejszej Umowy, zarządzania nią i jej monitorowania.
6. Podmiot Przetwarzający zapewni, że przetwarzać dane osobowe w jego imieniu będą wyłącznie osoby fizyczne posiadające upoważnienia, o których mowa art. 29 RODO i których dostęp jest niezbędny do realizacji celu, o którym mowa w § 2 ust. 4 niniejszej Umowy.
7. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
8. 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.
9. Podmiot przetwarzający zobowiązuje się do niezwłocznego i odpowiedniego rozpatrywania zapytań Administratora dotyczących przetwarzania danych zgodnie z niniejszą Umową.
10. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o wszelkich żądaniach udostępnienia danych przez upoważnione organy państwa.

§ 4
PRAWO KONTROLI

1. Administrator danych ma prawo kontroli przestrzegania przez Przetwarzającego zasad przetwarzania danych osobowych, tj. kontroli dokumentów, urządzeń i pomieszczeń związanych z przetwarzaniem danych osobowych, a także czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej Umowy.
2. Administrator danych realizować będzie prawo kontroli w miejscu przetwarzania danych osobowych w dni robocze w godzinach od 9.00 do 15.00 z minimum 3-dniowym uprzedzeniem Przetwarzającego.
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 RODO.

§ 5
DALSZE POWIERZENIE PRZETWARZANIA

1. Przetwarzający jest zobowiązany do niekorzystania z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej pisemnej zgody Administratora.
2. Podmiot przetwarzający zobowiązuje się złożyć do Administratora wniosek o udzielenie szczegółowej zgody co najmniej 14 dni przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego, wraz z informacjami niezbędnymi do tego, by Administrator mógł podjąć decyzję w sprawie zgody. Wykaz podmiotów podprzetwarzających, które Administrator upoważnia do przetwarzania danych osobowych stanowi Załącznik nr 1 do niniejszej Umowy. Strony są obowiązane do aktualizacji załącznika.

3. Niezależnie od obowiązku uzyskania zgody, o której mowa w ust. 1, przed rozpoczęciem korzystania z usług innego podmiotu przetwarzającego Przetwarzający przeprowadzi odpowiednią weryfikację, aby zapewnić, że inny podmiot przetwarzający jest w stanie zapewnić odpowiedni poziom ochrony danych osobowych.
4. Przetwarzający zobowiązuje się, iż w przypadku podpowierzenia przetwarzania danych dalszemu podmiotowi, Przetwarzający skorzysta z usług tego podmiotu w drodze umowy, która zapewni te same gwarancje i obowiązki ochrony danych jak w niniejszej Umowie.
5. Na wniosek Administratora podmiot przetwarzający przekazuje Administratorowi kopię umowy, o której mowa w ust. 4, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję.
6. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków ochrony danych przez inny podmiot przetwarzający, z którego usług korzysta. Podmiot przetwarzający powiadamia Administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.
7. Podmiot przetwarzający uzgodni w umowie 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 będzie miał prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.
8. 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.
9. Jeżeli Podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego zgodnie z ust. 4 w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V RODO, Administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V RODO za pomocą standardowych klauzul umownych zgodnie z art. 46 ust. 2 RODO, jeżeli spełnione są warunki stosowania tych klauzul.

§ 6
POMOC DLA ADMINISTRATORA

1. Podmiot przetwarzający zobowiązuje się niezwłocznie zawiadomić Administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że Administrator uprzednio wyrazi na to zgodę.
2. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą. Podmiot przetwarzający stosuje się przy tym do poleceń Administratora.
3. Podmiot przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO, w tym w szczególności dotyczących:
    a) bezpieczeństwa przetwarzania danych osobowych, w tym wdrożenia środków technicznych i organizacyjnych odpowiednich do wiążącego się z przetwarzaniem ryzyka przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

b) zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie Administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne
c) dokonywania oceny skutków dla ochrony danych,
d) skonsultowania się z organem nadzorczym, gdy ocena skutków dla ochrony danych wykaże wysokie ryzyko przetwarzania.

4. Podmiot przetwarzający pomaga Administratorowi za pomocą środków wskazanych w § 3 ust. 4, w zakresie wynikającym z celu powierzenia, o którym mowa w § 2 ust. 4 niniejszej Umowy.

§ 7

NARUSZENIE 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 RODO, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje Podmiot przetwarzający.
2. Jeżeli naruszenie ochrony danych dotyczy danych przetwarzanych przez Administratora, Podmiot przetwarzający wspomaga Administratora:
    a) przy zgłaszaniu naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych – w stosownych przypadkach i niezwłocznie po tym, jak Administrator dowiedział się o naruszeniu;
    b) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO 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 oraz 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;
    c) przy wypełnianiu - zgodnie z art. 34 RODO - obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
3. Jeżeli naruszenie ochrony danych dotyczy danych przetwarzanych przez Podmiot przetwarzający, zgłasza on 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.
4. Jeżeli przekazanie przez Podmiot przetwarzający wszystkich informacji równocześnie nie jest możliwe, pierwotne zgłoszenie Podmiotu przetwarzającego zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji, Podmiot przetwarzający uzupełnia je bez zbędnej zwłoki.

§ 8

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 („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 w innym celu niż wykonanie Umowy głównej, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa, niniejszej Umowy lub Umowy głównej.

§ 9
POSTANOWIENIA KOŃCOWE

1. Bez uszczerbku dla przepisów RODO, w przypadku gdy Podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszej Umowy, Administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy Podmiot przetwarzający zapewni zgodność z niniejszą Umową, lub Umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia Administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do postanowień niniejszej Umowy.
2. Administrator jest uprawniony do rozwiązania niniejszej Umowy, jeżeli:
    a) Administrator polecił zawieszenie przetwarzania danych osobowych przez Podmiot przetwarzający zgodnie z ust. 1, a Podmiot przetwarzający nie przywrócił zgodności z niniejszą Umową w terminie nie dłuższym niż jeden miesiąc od zawieszenia;
    b) Podmiot przetwarzający poważnie lub stale narusza niniejszą Umowę lub swoje obowiązki wynikające z RODO;
    c) Podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego organu nadzorczego dotyczącej jego obowiązków wynikających z niniejszej Umowy lub z RODO
3. Podmiot przetwarzający ma prawo rozwiązać niniejszą Umowę, jeżeli po zawiadomieniu Administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z § 3 ust. 2, Administrator nalega na wypełnienie polecenia.
4. W przypadku rozwiązania lub wygaśnięcia niniejszej Umowy, Podmiot przetwarzający zwraca Administratorowi wszelkie dane osobowe oraz niezwłocznie usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
5. Usunięcie danych osobowych, o którym mowa w ust. 4, oznacza zniszczenie danych lub modyfikację danych uniemożliwiającą ustalenie tożsamości osoby, której dane dotyczą.
6. W terminie 7 dni od powstania obowiązku usunięcia danych zgodnie z ust. 4 Podmiot Przetwarzający przekaże Administratorowi kopię protokołu potwierdzającego zniszczenie danych lub informację o obowiązku dalszego przechowywania danych ze wskazaniem okresu przechowywania i podstawy prawnej.
7. Podmiot przetwarzający zobowiązuje się zapewnić przestrzeganie odpowiednich postanowień niniejszej Umowy do czasu usunięcia danych.
8. Niniejsza Umowa jest integralną częścią Umowy głównej. Niniejsza Umowa zawarta zostaje na czas określony tj. na czas wykonywania Umowy głównej.
9. Niniejszą Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
10. W sprawach nieuregulowanych niniejszą Umową zastosowanie będą miały przepisy Kodeksu cywilnego i RODO.

11. W przypadku, gdy niniejsza Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
12. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej w postaci aneksu pod rygorem nieważności.
13. Wszelkie spory wynikające z niniejszej umowy strony poddadzą pod rozstrzygnięcie Sądu powszechnego właściwego miejscowo dla siedziby Administratora danych.

_____	_____
Administrator danych	Podmiot przetwarzający

Załączniki:

- Zał. 1 – wykaz podmiotów podprzetwarzających zaakceptowanych przez Administratora

Wykaz podmiotów podprzetwarzających
zaakceptowanych przez Uniwersytet Ekonomiczny w Krakowie

Administrator zezwolił na korzystanie przez Podmiot przetwarzający z usług następujących podmiotów podprzetwarzających:

1.
Imię i nazwisko lub nazwa: .....

Adres: .....

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

.....

Opis przetwarzania: .....

Zakres odpowiedzialności: .....

2.
Imię i nazwisko lub nazwa: .....

Adres: .....

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

.....

Opis przetwarzania: .....

Zakres odpowiedzialności: .....

3.

Imię i nazwisko lub nazwa: .....

Adres: .....

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

Opis przetwarzania: .....

Zakres odpowiedzialności: .....