**Umowa powierzenia przetwarzania danych osobowych**

zawarta dnia ………………. pomiędzy:

**Akademią Nauk Stosowanych im. J.A. Komeńskiego
ul. Mickiewicza 5,
64-100 Leszno**

**reprezentowaną przez:**

**Dr Janusza Połę, prof. ANS - Rektora**

Zwanym w dalszej części umowy **„ Administratorem”**
a

**…………………**

**ul. ……………………………;
……………………………………**

Zwanym w dalszej części umowy „**Podmiotem przetwarzającym”**

zaś wspólnie **„Stronami”**

W związku z zawarciem w dniu …………………………. umowy zwanej dalej „Umową główną”, której przedmiotem są czynności związane z świadczeniem stałej usługi ochrony mienia
i osób fizycznych w Akademii Nauk Stosowanych im. J. A. Komeńskiego w Lesznie. Strony postanawiają co następuje:

**§ 1**

**Powierzenie przetwarzania danych osobowych**

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 *R*ozporządzenia 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(zwane dalej „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu do przetwarzania.
3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający w celu realizacji zawartej pomiędzy stronami umowy z dnia …………………………………………………………………………………………………………………………………….Podmiot przetwarzający oświadcza, że przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – 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 to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

 **§2**

**Zakres i cel przetwarzania danych**

1. Administrator powierza Podmiotowi przetwarzającemu na podstawie umowy dane pracowników, kontrahentów, użytkowników biblioteki, mieszkańców domu studenta. obejmujące następujące struktury danych: nazwiska i imiona, stanowiska pracowników, pełniona funkcja, wizerunek. Administrator oświadcza, iż przetwarzanie danych osobowych w ramach niniejszej umowy odnosi się do kategorii odczytu, przechowywania, usuwania danych osobowych.
2. Powierzone do przetwarzania dane osobowe mogą być przetwarzane wyłącznie w celu i zakresie adekwatnym do prawidłowej realizacji Umowy głównej.
3. Podmiot przetwarzający nie może powierzyć danych osobowych objętych niniejszą umową do dalszego przetwarzania podwykonawcom bez uzyskania pisemnej zgody Administratora danych.

**§3**

**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. Wdrażając środki organizacyjne i techniczne, o których mowa powyżej, Podmiot przetwarzający:
3. przestrzega wytycznych Administratora w zakresie sposobu zabezpieczenia procesów przetwarzania danych osobowych zgodnie z przepisami Rozporządzenia oraz innymi obowiązującymi przepisami prawa. Minimalne gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych wymaganych przez Administratora stanowi załącznik nr 1 i załącznik nr 2 do Umowy;
4. powinien uwzględnić stan wiedzy technicznej oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których dane osobowe będzie przetwarzał na podstawie Umowy.
5. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
6. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane
w celu realizacji niniejszej umowy.
7. 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, jak i po jego ustaniu.
8. Podmiot przetwarzający po zakończeniu świadczenia usług związanych
z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
9. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi
w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
10. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 godzin .

**§4**

**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 3 dniowymjego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym
niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.  **§5**

**Dalsze powierzenie danych do przetwarzania**

1. Podmiot przetwarzający nie może powierzyć danych osobowych objętych niniejszą umową do dalszego przetwarzania podwykonawcom bez uzyskania pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie
na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada
na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych
o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji
z uwagi na ważny interes publiczny.

**§ 6**

**Odpowiedzialność Podmiotu przetwarzającego**

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych
przez Administratora danych.

 **§7**

**Czas obowiązywania umowy**

1. Niniejsza umowa obowiązuje od dnia 1.10.2024r. do dnia 31.03.2026r. **§8**

**Rozwiązanie umowy**

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
2. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
3. przetwarza dane osobowe w sposób niezgodny z umową;
4. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

**§9**

**Postanowienia końcowe**

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej

ze stron.

1. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
2. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Administrator Przetwarzający

Złącznik nr 1 do Umowy powierzenia z dnia ……………………………………………….

|  |
| --- |
| **WERYFIKACJA/ANALIZA****ŚRODKÓW ZABEZPIECZEŃ ORGANIZACYJNYCH i TECHNICZNYCH ZASTOSOWANYCH PRZEZ PODMIOT PRZETWAZRAJĄCY**  |
| **ADMINISTRATOR DANYCH** | **Akademia Nauk Stosowanych im. J.A. Komeńskiego ul. Mickiewicza 5,64-100 Leszno****Reprezentowana przez:****Dr Janusza Połę, prof. ANS - Rektora**  |
| **PODMIOT PRZETWARZAJĄCY** | **………………………………………………..****…………………………………………………****………………………………………………..** |
| **Grupa zabezpieczeń** | **Opis zabezpieczeń** | Uzupełnia Przetwarzający: |
| Środki organizacyjne | 1. Zapewniono kontrolę nad dostępem do Danych osobowych, w szczególności poprzez: |   |
|   | 1) wyznaczenie osób upoważnionych do przetwarzania danych osobowych na polecenie Administratora i wydanie imiennych upoważnień do przetwarzania danych osobowych, |   |
|   | 2) zapewnienie, że osoby posiadające upoważnienia, o których mowa w pkt 1 zobowiązały się do zachowania tajemnicy. |   |
|   | 2. Zapewniono szkolenia z zakresu bezpieczeństwa przetwarzania danych osobowych dla osób biorących udział w procesie przetwarzania. |   |
|   | 3. Przyjęto i wdrożono polityki ochrony danych, w tym polityki bezpieczeństwa danych w systemach informatycznych. |   |
|   | 4. Prowadzony jest rejestr kategorii czynności przetwarzania danych. |   |
|   | 5. Przyjęto i wdrożono procedurę związaną z reagowaniem na naruszenia ochrony danych, w tym prowadzony jest rejestr naruszeń ochrony danych osobowych. |   |
|   | 6. Prowadzona jest analiza ryzyka w zakresie przetwarzania danych osobowych. |   |
| **WYMAGANIA RODO** | Czy podmiot przetwarzający spełnia wymagania RODO z art. 24 RODO? |  |
| Czy podmiot przetwarzający spełnia wymagania RODO z art. 32 RODO? |  |

 **PODPIS OSOBY REPREZENTUJĄCEJ PODMIOT PRZETWARZAJĄCY**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Złącznik nr 2 do Umowy powierzenia z dnia …………………………………………….

***MINIMALNE GWARANCJE WDROŻENIA ODPOWIEDNICH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH PRZEZ PODMIOT PRZETWARZAJĄCY***

1. Obszar, w którym przetwarzane są dane osobowe, należy zabezpieczyć przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. W przypadku realizacji usług poza wskazanym obszarem
z wykorzystaniem urządzeń przenośnych, należy zabezpieczać je, stosując środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
2. System informacyjny należy chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, obejmującym przykładowo:
3. kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
4. kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
5. System powinien zostać wyposażony w mechanizm filtrowania połączeń wchodzących i wychodzących (firewall – zapora sieciowa).
6. System informatyczny musi zostać wyposażony w mechanizmy ochrony antywirusowej. Wszystkie pliki muszą być testowane oprogramowaniem antywirusowym.
7. Każdy komputer powinien mieć założone zabezpieczenie uniemożliwiające osobom nieupoważnionym zmianę konfiguracji komputera.
8. Załączniki do poczty elektronicznej nie powinny być otwierane, jeśli zachodzi podejrzenie, że zostały wysłane z niezaufanego źródła.
9. Należy stosować środki ochrony kryptograficznej wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
10. W systemie informatycznym służącym do przetwarzania danych osobowych muszą istnieć odpowiednie mechanizmy kontroli dostępu do danych. Należy wziąć pod uwagę stosowanie: tworzenie i usuwanie kont, ich czasowe lub trwałe blokowanie, nadawanie haseł i ich zmianę oraz nadawanie i wycofywanie uprawnień, raportowanie wszystkich istotnych operacji zawiązanych z zarządzaniem uprawnieniami, generowane
z perspektywy czasu, konta, roli lub operacji.
11. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają
co najmniej dwie osoby, wówczas należy zapewnić, aby:
12. w systemie rejestrowany był dla każdego użytkownika odrębny identyfikator,
13. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora
i dokonaniu uwierzytelnienia.
14. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
15. Systemy informatyczne muszą być zabezpieczone w szczególności przed:
16. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
17. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
18. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczane przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących
do przetwarzania danych.
19. Kopie zapasowe:
20. należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
21. muszą być usuwane niezwłocznie po ustaniu ich użyteczności.
22. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
23. likwidacji – pozbawia się wcześniej zapisu danych, a w przypadku, gdy nie jest
to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
24. przekazanie innemu podmiotowi – pozbawia się wcześniej zapisu danych, w sposób uniemożliwiający ich odzyskanie,
25. naprawy – pozbawia się wcześniej zapisu danych w sposób uniemożliwiający
ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.
26. Przetwarzający zobowiązany jest do monitorowania wdrożonych środków zabezpieczenia systemu informatycznego.
27. Przetwarzający posiada wiedzę z zakresu przepisów regulujących przetwarzanie danych osobowych i jest zobowiązany do uzupełniania swojej wiedzy z tego zakresu w przypadku zmian w przepisach.
28. Przetwarzający ma obowiązek zapoznania swoich pracowników, którzy mają być uprawnieni do przetwarzania danych osobowych, z przepisami dotyczącymi danych osobowych i odpowiedzialnością za ochronę tych danych.
29. Należy prowadzić dokumentację ustalającą zasady ochrony danych osobowych.

**Administrator Przetwarzający**

**………………………………… …………………………..**