Załącznik
do zarządzenia Rektora Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie Nr ZR/2024/0075 z dnia 17.10.2024 r.

Polityka Bezpieczeństwa Informacji w zakresie danych osobowych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie

§ 1
Wyjaśnienie terminów używanych w dokumencie Polityki Bezpieczeństwa

Ilekroć w Polityce Bezpieczeństwa Informacji w zakresie danych osobowych jest mowa o:

1) **Danych osobowych** – rozumie się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2) **Danych biometrycznych** – dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
3) **Danych dotyczących zdrowia** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
4) **Danych genetycznych** – dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
5) **Przetwarzaniu** – rozumie się operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
6) **Ograniczeniu przetwarzania** – rozumie się oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
7) **Profilowaniu** - rozumie się dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
8) **Pseudonimizacji** - rozumie się przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi

9) **Administratorze danych osobowych (ADO)** - rozumie się przez to Administratora danych – Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie;
10) **Inspektorze ochrony danych osobowych (IODO)** - rozumie się przez to osobę, której Administrator danych osobowych powierzył pełnienie obowiązków Inspektora ochrony danych osobowych;
11) **Administratorze systemu informatycznego (ASI)** - rozumie się przez to pracowników Działu Informatyki Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie, administrujący systemami informatycznymi w imieniu Administratora danych osobowych;
12) **Osobie upoważnionej do przetwarzania danych osobowych** - rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Rektora;
13) **Użytkowniku** – rozumie się każdą upoważnioną osobę, która przetwarza dane osobowe w ramach wykonywanych zadań służbowych;
14) **Pracowniku** – rozumie się osoby pozostające w stosunku pracy, jak również osoby współpracujące z administratorem danych osobowych na podstawie umów cywilnoprawnych, stażystów, praktykantów, wolontariuszy;
15) **Kierownika działu** – rozumie się dyrektora lub kierownika danego działu, dziekanatu lub innej, niebędącej wydziałem jednostki organizacyjnej;
16) **Podmiocie przetwarzającym** – rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora danych osobowych;
17) **Odbiorcy** – rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
18) **Stronie trzeciej -** rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia Administratora danych osobowych lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
19) **Zgodzie osoby, której dane dotyczą** – rozumie się dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalającego na przetwarzanie dotyczących jej danych osobowych;
20) **Incydencie ochrony danych osobowych** – rozumie się naruszenie bezpieczeństwa danych osobowych nie skutkujące wystąpieniem wysokiego ryzyka naruszenia praw lub wolności osób;
21) **Naruszeniu ochrony danych osobowych** - rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, skutkujące wysokim ryzykiem naruszenia praw lub wolności osób;
22) **Systemie informatycznym** – rozumie się zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
23) **Usuwaniu danych** – rozumie się zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

24) **Rozporządzeniu (RODO)** – rozumie się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) (Dz.U. UE z 2016 roku, nr L 119, poz. 1);
25) **Ustawie** – rozumie się ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 178 z późn. zm.);
26) **Organie nadzorczym** – rozumie się Prezesa Urzędu Ochrony Danych Osobowych;
27) **2FA** – rozumie się uwierzytelnienie dwuskładnikowe;
28) **Centralny System Logowania** – rozumie się system oparty o metodę jednokrotnego logowania (tzw. SSO).

§ 2
Postanowienia ogólne

1. Niniejszy dokument powstał w związku z wejściem w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 osobowych, zwanego dalej „Rozporządzenie (RODO) „) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 178 z późn. zm.). Powyższe przepisy nakładają również na uczelnie szereg obowiązków związanych z ochroną danych osobowych, zatem niezbędne okazało się wprowadzenie uregulowań w tym zakresie w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie, zwanym dalej „Uczelnią”.
2. Niniejszy dokument określa zasady przetwarzania danych osobowych oraz środki ochrony danych osobowych, w tym pod kątem zabezpieczeń stosowanych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie.
3. Głównym celem Polityki Bezpieczeństwa Informacji w zakresie ochrony danych osobowych, zwanej dalej „PBI”, jest wprowadzenie organizacyjnych, fizycznych i logistycznych procedur dotyczących zabezpieczeń przetwarzanych danych oraz systematyczne edukowanie uczestników procesów ich przetwarzania.
4. Ponadto, celem opracowania i wdrożenia Polityki Bezpieczeństwa Informacji w zakresie ochrony danych osobowych jest osiągnięcie poziomu organizacyjnego i technicznego, który:
   1) będzie gwarantem pełnej ochrony osób, których dane dotyczą oraz ciągłości procesu ich przetwarzania;
   2) zapewni zachowanie poufności informacji chronionych oraz legalności, przejrzystości, rzetelności, celowości, adekwatności, prawidłowości, czasowości, integralności i poufności przetwarzania danych osobowych osób fizycznych;
   3) zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach i formach jej przetwarzania;
   4) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji i danych osobowych, wynikających z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie;
   5) zapewni gotowość do podjęcia działań w sytuacjach zagrożenia dla bezpieczeństwa Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie, jego interesów oraz posiadanych i powierzonych mu informacji i danych osobowych.

5. Polityka Bezpieczeństwa Informacji w zakresie ochrony danych osobowych, ma służyć skutecznej ochronie danych osobowych przetwarzanych przez Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie zarówno metodami tradycyjnymi, jak i z wykorzystaniem systemów informatycznych. Należy przez to rozumieć w szczególności ochronę przed udostępnieniem danych osobowych osobom nieupoważnionym oraz zapewnienie integralności danych poprzez ścisłe przestrzeganie wymogów wynikających z obowiązujących przepisów prawa.

Podmioty odpowiedzialne za przetwarzanie danych osobowych

§ 3
Administrator Danych Osobowych (ADO)

1. Administratorem danych osobowych jest Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie. Uczelnia może występować także w roli współadministratora albo podmiotu przetwarzającego dane osobowe na podstawie zawartej umowy powierzenia przetwarzania danych osobowych.
2. Administratora danych osobowych reprezentuje Rektor zgodnie z zakresem kompetencji wynikających z przepisów ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. 2023 r. poz. 742 z późn. zm.) oraz Statutu Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie.
3. Administrator danych osobowych wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z powszechnie obowiązującymi przepisami prawa, w tym przepisami Rozporządzenia (RODO) i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
4. Obowiązki Administratora danych osobowych w zakresie ochrony danych osobowych, obejmują w szczególności:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z przepisami powszechnie obowiązującymi;
   2) zapewnienie przetwarzania danych zgodnie z prawem oraz uregulowaniami Polityki i innymi dokumentami wewnętrznymi;
   3)zapewnienie adekwatnych do zagrożeń i kategorii przetwarzanych danych osobowych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w Uczelni;
   4) dokonywanie oceny skutków dla ochrony danych po konsultacji z Inspektorem ochrony danych osobowych lub Administratorem systemów informatycznych;
   5) powołanie Inspektora ochrony danych osobowych;
   6) prowadzenie we współpracy z Inspektorem ochrony danych osobowych Rejestru czynności przetwarzania danych;
   7) prowadzenie we współpracy z Inspektorem ochrony danych osobowych Rejestru kategorii czynności przetwarzania w razie przetwarzania danych osobowych w imieniu i na rzecz innego Administratora danych osobowych;
   8) wyznaczenie Administratora Systemów Informatycznych;
   9) wydawanie i cofanie upoważnień do przetwarzania danych osobowych;
   10) nadzór nad bezpieczeństwem danych osobowych.

§ 4
Inspektor Ochrony Danych Osobowych (IODO)

1. Inspektor ochrony danych osobowych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań.

2. Inspektor ochrony danych osobowych może być pracownikiem administratora lub wykonywać zadania na podstawie umowy o świadczenie usług. Inspektor ochrony danych osobowych może wykonywać inne zadania i obowiązki. Administrator danych osobowych zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
3. Inspektor ochrony danych osobowych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
4. Administrator danych osobowych publikuje dane kontaktowe inspektora ochrony danych osobowych i zawiadamia o nich organ nadzorczy.
5. Do zadań Inspektora ochrony danych osobowych należy w szczególności:

1) informowanie Administratora danych osobowych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia (RODO), innych przepisów Unii oraz krajowych przepisów dotyczących ochrony danych osobowych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania przepisów Rozporządzenia (RODO), innych przepisów Unii oraz krajowych przepisów dotyczących ochrony danych osobowych, a także polityk ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych oraz podejmowania działań zwiększających świadomość w operacjach przetwarzania danych osobowych;
3) udzielanie na żądanie Administratora danych osobowych zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania zgodnie z art. 35 Rozporządzenia (RODO);
4) opiniowanie projektów, zarządzeń i innych dokumentów, w zakresie dotyczącym danych osobowych;
5) wspieranie Administratora danych osobowych w prowadzeniu Rejestru czynności przetwarzania danych prowadzenie (przy współpracy z Kierownikami Działów), którego wzór stanowi załącznik nr 1 do Polityki Bezpieczeństwa Informacji;
6) wspieranie Administratora danych osobowych w prowadzeniu Rejestru kategorii czynności przetwarzania danych, którego wzór stanowi załącznik nr 2 do Polityki Bezpieczeństwa Informacji;
7) prowadzenie Rejestru umów powierzenia przetwarzania danych osobowych, którego wzór stanowi załącznik nr 3 do Polityki Bezpieczeństwa Informacji;
8) prowadzenie Rejestru udostępnień danych osobowych, którego wzór stanowi załącznik nr 4 do Polityki Bezpieczeństwa Informacji;
9) prowadzenie Rejestru incydentów dotyczących bezpieczeństwa ochrony danych osobowych, którego wzór stanowi załącznik nr 5 do Polityki Bezpieczeństwa Informacji;
10) przekazywanie Administratorowi danych osobowych informacji dotyczących naruszeń bezpieczeństwa ochrony danych;
11) przeprowadzanie kontroli działań jednostek organizacyjnych Administratora danych osobowych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
12) współpraca z Organem nadzorczym;
13) pełnienie funkcji punktu kontaktowego dla Organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia (RODO) oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

§ 5
Administrator Systemów Informatycznych (ASI)

1. W celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w systemach teleinformatycznych, pracownicy Działu Informatyki Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie administrują oraz zarządzają systemami informatycznymi (ASI).
2. W zakresie realizacji swoich zadań, Administrator systemów informatycznych współpracuje z Inspektorem ochrony danych osobowych.
3. Do uprawnień i obowiązków Administratora systemów informatycznych w szczególności należą:

1) nadawanie szczegółowego dostępu pracownikom upoważnionym do przetwarzania danych osobowych przez Administratora danych osobowych do systemów informatycznych, w szczególności przydzielenie tym pracownikom pierwszych haseł oraz uprawnień do poszczególnych funkcji właściwych im systemów informatycznych;
2) zapoznanie osób zatrudnionych przy przetwarzaniu danych osobowych z zasadami bezpiecznego korzystania z komputera i obsługi systemów informatycznych;
3) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
4) stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo systemów informatycznych;
5) wykonywanie czynności związanych z funkcjonowaniem i modernizacją systemów informatycznych;
6) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych znajdujących się w systemach informatycznych. Spis systemów informatycznych, w których przetwarzane są dane osobowe stanowi załącznik nr 6 do Polityki Bezpieczeństwa Informacji;
7) prowadzenie ewidencji oprogramowania wykorzystywanego w Uczelni;
8) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych.

§ 6
Osoby upoważnione do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych i obsługi systemów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby mające upoważnienie wydane przez Administratora danych osobowych w obszarach ich odpowiedzialności.
2. Upoważnienie do przetwarzania danych osobowych, o którym mowa w ust. 1 wydaje oraz cofa Rektor zgodnie z zakresem kompetencji wynikających z przepisów ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. 2023 r. poz. 742 z późn. zm.) oraz Statutu Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie.
3. Upoważnienie do przetwarzania danych osobowych, wydawane jest w dwóch egzemplarzach, z których jeden jest przekazywany osobie upoważnionej do przetwarzania danych, zaś drugi przechowywany jest w Dziale Spraw Osobowych Uczelni. Kserokopia upoważnienia do przetwarzania danych osobowych w systemach informatycznych jest przekazywana przez pracowników Działu Spraw Osobowych do Administratora systemów informatycznych w celu nadania uprawnień w systemach informatycznych.
4. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji, wygaśnięcie albo rozwiązanie umowy cywilnoprawnej bądź cofnięcie upoważnienia przez

Administratora danych osobowych powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

5. Informacja o wygaśnięciu upoważnienia do przetwarzania danych osobowych, w sytuacjach o, których mowa w ust. 4, przekazywana jest niezwłocznie Administratorowi systemów informatycznych przez pracowników Działu Spraw Osobowych, w celu zablokowania dostępu do systemów informatycznych.
6. Wzór upoważnienia do przetwarzania danych osobowych wraz ze wzorem oświadczenia osoby upoważnianej do zachowania tajemnicy stanowią załączniki nr 7 do Polityki Bezpieczeństwa Informacji.
7. Ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wydanych upoważnień prowadzi w wersji elektronicznej Dział Spraw Osobowych, do którego dostęp posiada Inspektor ochrony danych osobowych oraz Administrator systemów informatycznych, którego wzór stanowi załącznik nr 8 do Polityki Bezpieczeństwa Informacji.

Przetwarzanie danych osobowych

§ 7
Zasady przetwarzania danych osobowych

1. Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie przetwarza dane osobowe zgodnie z określonymi celami przy spełnieniu przynajmniej jednego z poniższych warunków:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze danych osobowych;
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi danych osobowych;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora danych osobowych lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.
2. Zakres przetwarzania danych osobowych przez Administratora danych osobowych określają przepisy prawa oraz umowy zawierane z podmiotami zewnętrznymi.

§ 8

1. Dane osobowe przetwarzane w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie mogą być pozyskiwane:
   1) bezpośrednio od osób, których te dane dotyczą;
   2) z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Zbierane dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane;
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, chyba, że przepisy szczególne stanowią inaczej.

§ 9

1. Przetwarzanie szczególnych kategorii danych, które określają:
   1) pochodzenie rasowe lub etniczne,
   2) poglądy polityczne,
   3) przekonania religijne lub światopoglądowe,
   4) przynależność związkową, a także przetwarzanie danych genetycznych, biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub
   5)dane dotyczące zdrowia, seksualności lub orientacji seksualnej jest zabronione, z zastrzeżeniem ust. 2.
2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:
   1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo krajowe przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
   2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora danych osobowych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem krajowym;
   3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
   4) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń;
   5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
   6) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie przepisów prawa;
   7) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych oraz do celów statystycznych.

§ 10

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, wówczas osoba działająca z upoważnienia Administratora danych osobowych podczas zbierania danych osobowych podaje jej następujące informacje:
   1) tożsamość i dane kontaktowe Administratora danych osobowych,
   2) dane kontaktowe Inspektora ochrony danych osobowych,
   3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
   4) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców.

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych podaje się osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
   1) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   2) informacje o prawie do żądania od Administratora danych osobowych dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   3) informację o prawie wniesienia skargi do Organu nadzorczego;
   4) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje odmowy podania.
3. Jeżeli Administrator danych osobowych planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
4. Administrator danych osobowych zbierając dane osobowe od osoby, której dane dotyczą winien przekazać informacje, o których mowa w ust. 1 i 2, realizując tym samym obowiązek informacyjny wynikający z art. 13 Rozporządzenia (RODO).
5. Wzór przykładowej klauzuli informacyjnej stanowi załącznik nr 9 do niniejszej Polityki. Dopuszczalne jest stosowanie innych wzorów klauzul po uprzednim ustaleniu i uzgodnieniu z Inspektorem ochrony danych osobowych.
6. Odpowiedzialni za poinformowanie osób, o których mowa w ust. 1 i odebranie od nich potwierdzeń zapoznania się z informacjami są kierownicy danego działu.

§ 11
Prawa osób, których dane dotyczą

1. Wszystkie osoby, których dane przetwarza się w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie, mają prawo:

   1) uzyskać od Administratora danych osobowych potwierdzenie czy jej dane osobowe są przetwarzane, a jeżeli ma to miejsce, są uprawnione do uzyskania informacji w następującym zakresie:
   a) cele przetwarzania;
   b) kategorie danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania od Administratora danych osobowych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacje o prawie wniesienia skargi do Organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;
h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu 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) żądać od Administratora danych osobowych niezwłocznego sprostowania jej danych osobowych, jeśli są nieprawidłowe;
3) żądać – z uwzględnieniem celów przetwarzania – uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia;
4) żądać od Administratora danych osobowych niezwłocznego usunięcia jej danych osobowych, jeżeli zachodzi jedna z następujących okoliczności:
a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie (zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) Rozporządzenia RODO i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw (zgodnie z art. 21 ust. 1 Rozporządzenia RODO) wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby marketingu bezpośredniego (zgodnie z art. 21 ust. 2 Rozporządzenia RODO);
d) dane osobowe są lub były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie krajowym;
f) dane osobowe zostały zebrane w związku z oferowaniem bezpośrednio dziecku usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 Rozporządzenia RODO.
5) kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych;
6) żądać od Administratora danych osobowych ograniczenia przetwarzania w następujących przypadkach:
a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający Administratorowi danych osobowych sprawdzić prawidłowość tych danych;
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) Administrator danych osobowych nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 Rozporządzenia RODO wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora danych osobowych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
7) otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi danych osobowych oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora danych osobowych, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) Rozporządzenia RODO lub art. 9 ust. 2 lit. a) Rozporządzenia RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) Rozporządzenia RODO oraz b) przetwarzanie odbywa się w sposób zautomatyzowany;

8) w dowolnym momencie wnieść sprzeciw wobec dotyczących jej danych osobowych (zgodnie z art. 21 Rozporządzenia RODO);

9) do tego, aby nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa – z wyłączeniem sytuacji, gdy ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem danych osobowych;

b) jest dozwolona prawem Unii lub prawem krajowym i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

2. Administrator danych osobowych bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie ust. 1. Termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

3. Wzór informacji o danych osobowych przetwarzanych przez Administratora danych osobowych stanowi załącznik nr 10 do Polityki Bezpieczeństwa Informacji.

4. „Prawo do bycia zapomnianym" nie ma zastosowania w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie w zakresie, w jakim przetwarzanie danych osobowych jest niezbędne:

1) do wywiązania się przez Administratora danych osobowych z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa polskiego;

2) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;

3) do celów ustalenia, dochodzenia roszczeń lub ochrony praw.

§ 12
Udostępnianie danych osobowych

1. Dane osobowe udostępnia się wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, a udostępnienie danych nie narusza praw i wolności osób, których udostępniane dane dotyczą. Udostępnianie danych osobowych instytucjom i osobom spoza Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie może odbywać się wyłącznie po uprzednim uzgodnieniu z Inspektorem ochrony danych osobowych.
2. Podmiot zwracający się z wnioskiem o udostępnienie danych osobowych winien wskazać cel lub podstawę prawną udostępnienia.
3. Inspektor ochrony danych osobowych prowadzi Rejestr udostępnianych danych osobowych, w którym fakt udostępnienia danych jest również każdorazowo odnotowywany.

§ 13
Udostępnianie informacji publicznej

1. Udostępnienie informacji publicznej na wniosek w trybie ustawy o dostępie do informacji publicznej następuje bez zbędnej zwłoki, nie później jednak niż w terminie 14 dni od złożenia wniosku.

2. Jeżeli realizacja wniosku wymaga dłuższego okresu przygotowania, powiadamia się pisemnie wnioskodawcę o wydłużeniu terminu załatwienia wniosku, nie dłuższym niż 2 miesiące od dnia złożenia wniosku.
3. Udostępnianie informacji publicznej na wniosek następuje w sposób i w formie zgodnej z wnioskiem, chyba że środki techniczne, którymi Administrator danych osobowych dysponuje nie umożliwiają udostępnienia informacji w sposób i w formie określonej we wniosku.
4. Dostęp do informacji publicznej jest ograniczony w przypadkach:
   a) informacji niejawnej (tajemnicy państwowej i służbowej),
   b) informacji stanowiącej tajemnicę ustawowo chronioną (tajemnicę zawodową lub jednostki organizacyjnej),
   c) tajemnicy przedsiębiorcy,
   d) ze względu na ochronę danych osobowych lub prywatność osoby fizycznej.
5. Odmowa udostępnienia informacji publicznej oraz umorzenie postępowania o udostępnienie informacji publicznej następuje w drodze decyzji wydanej zgodnie z Kodeksem postępowania administracyjnego przez Rektora bądź inną osobę upoważnioną.

§ 14
Powierzenie przetwarzania danych osobowych

1. W celu powierzenia podmiotom zewnętrznym przetwarzania danych osobowych będących w posiadaniu Administratora danych osobowych, zawierane są pisemne umowy powierzenia przetwarzania danych osobowych. Wzór umowy stanowi załącznik nr 11 do Polityki Bezpieczeństwa Informacji.
2. Umowa powierzenia przetwarzania danych osobowych winna określać:
   a) przedmiot przetwarzania,
   b) czas trwania przetwarzania,
   c) charakter i cel przetwarzania,
   d) rodzaj danych osobowych,
   e) kategorię osób, których dane dotyczą,
   f) obowiązki i prawa administratora,
   g) obowiązki podmiotu przetwarzającego.
3. Uprawnionym do zawierania umów powierzenia przetwarzania danych osobowych jest Rektor bądź Pełnomocnik Rektora ds. praktyk studenckich posiadający pełnomocnictwo do zawierania umów w zakresie praktyk studenckich.
4. Wszystkie umowy dotyczące powierzenia danych osobowych, powinny zostać przed podpisaniem zaopiniowane przez Inspektora ochrony danych osobowych.
5. Ewidencję zawartych umów powierzenia przetwarzania danych osobowych prowadzi Inspektor ochrony danych osobowych.
6. Egzemplarze zawartych umów powierzenia przetwarzania danych osobowych przechowuje Inspektor ochrony danych osobowych.

§ 15
Obszar przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych) oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).

2. Obszar przetwarzania danych osobowych określony jest w Polityce Bezpieczeństwa Informacji jako obszar o szczególnym znaczeniu dla funkcjonowania Uczelni.
3. Wykaz budynków, pomieszczeń oraz części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe stanowi załącznik nr 12 do Polityki Bezpieczeństwa Informacji.

§ 16
Zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

Pracownicy przetwarzający dane osobowe, niezależnie od celu i sposobu przetwarzania, są zobowiązani przestrzegać następujących zasad:

1) mogą przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora danych osobowych w upoważnieniu i tylko w celu wykonywania nałożonych na te osoby obowiązków;

2) są zobowiązane zachować poufność danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie poufności danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora danych osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji, albo po wygaśnięciu lub rozwiązaniu umowy cywilnoprawnej;

3) są zobowiązane do zapoznania się z przepisami prawa dotyczącymi ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa Informacji, w zakresie niezbędnym do stosowania w odniesieniu do ochrony danych osobowych;

4) są zobowiązane korzystać z systemów informatycznych oraz środowiska informatycznego w sposób zgodny ze wskazówkami zawartymi w Instrukcji korzystania z urządzeń informatycznych, w szczególności komputerów, drukarek oraz oprogramowania komputerowego, a także wewnętrznej sieci komputerowej w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie, stanowiącej załącznik nr 13 do Polityki Bezpieczeństwa Informacji. Każdy pracownik potwierdza na piśmie znajomość wyżej wymienionej Instrukcji w momencie uzyskania dostępu do urządzeń oraz systemów informatycznych;

5) są zobowiązane do postępowania zgodnie z zasadami określonymi w Instrukcji Zarządzania Systemami Informatycznymi, stanowiącej załącznik nr 14 do Polityki Bezpieczeństwa Informacji;

6) są zobowiązane zabezpieczać przetwarzane dane osobowe przed dostępem osób nieupoważnionych, zgodnie z zasadami określonymi w § 17 Polityki Bezpieczeństwa Informacji. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę

tych danych osobowych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu;

7) są zobowiązane powiadomić Inspektora ochrony danych osobowych o wszelkich incydentach albo naruszeniach dotyczących przetwarzania danych osobowych oraz podjąć konieczne działania dotyczące ograniczenia skutków naruszenia;

8) są zobowiązane stosować polecenia Administratora danych osobowych, Inspektora ochrony danych osobowych oraz Administratora systemów informatycznych w zakresie ochrony danych osobowych.

§ 17

1. Za bezpieczeństwo przetwarzania danych osobowych, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do tych danych.
2. W miejscu przetwarzania danych osobowych pracownicy zobowiązani są do stosowania zasad tzw. „czystego biurka" oraz „czystego ekranu" stanowiących załącznik nr 15 do niniejszej Polityki Bezpieczeństwa Informacji. Za realizację powyższych zasad odpowiedzialny jest na swym stanowisku każdy z pracowników.
3. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
4. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia.
5. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
6. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.
7. Pracownicy realizując zadania o charakterze służbowym powinni posługiwać się adresem e-mailowym założonym w domenie Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie (afm.edu.pl lub uafm.edu.pl). Korzystanie w celach służbowych z prywatnych adresów e-mailowych jest dopuszczalne wyłącznie przez pracowników wykonujących obowiązki dydaktyczne na podstawie pisemnej zgody na przetwarzanie i udostępnienie adresu e-mail. Wzór zgody na przetwarzanie i udostępnienie prywatnego adresu e-mail stanowi załącznik nr 16 do Polityki Bezpieczeństwa Informacji.
8. Pracownicy podczas wysyłania zewnętrznej korespondencji mailowej adresowanej do wielu odbiorców powinni umieszczać adresy e-mailowe w polu „ukryte do wiadomości" (UDW), a wysyłając wiadomość za pośrednictwem Webmail „dodaj bcc" (ukryta kopia), z wyjątkiem służbowej korespondencji mailowej, z której charakteru wynika konieczność ujawnienia odbiorców danej wiadomości.

9. Pracownicy podczas wysyłania zewnętrznej korespondencji mailowej, do której załączony jest plik zawierający dane osobowe, w szczególności dane osobowe szczególnej kategorii, dane osobowe dotyczące wielu osób, zobowiązani są do zabezpieczenia pliku poprzez jego szyfrowanie (plik zabezpieczony hasłem).
10. Obieg dokumentów powinien być zgodny z obowiązującymi w Uczelni zasadami z zachowaniem regulacji wymaganych ochroną danych osobowych.
11. Każdy dokument przeznaczony lub adresowany do pracownika powinien być mu wręczony przez innego upoważnionego pracownika osobiście i nie może być pozostawiony w miejscu, w którym osoby nieupoważnione miałaby do niego dostęp. Dotyczy to w szczególności wszystkich pism niezależnie od rodzaju zawartych w nich informacji, dokumentów studentów (listy studentów, karty zaliczeniowe/egzaminacyjne, prace zaliczeniowe, prace dyplomowe itp.), przydziałów zajęć, umów (niezależnie od ich rodzaju) oraz dokumentów niewymienionych, a które mogą zawierać dane osobowe. Przekazując dokumenty mogące zawierać dane osobowe należy przenosić je w sposób zapobiegający ich kradzieży, zgubieniu lub utracie.
12. Udostępnienie studentom telefonicznie informacji zawierających dane osobowe jest dopuszczalne wyłącznie jeżeli tożsamość osoby, z którą prowadzona jest rozmowa została pozytywnie zweryfikowana za pośrednictwem imienia i nazwiska, numeru albumu, daty urodzenia. Jeżeli istnieją wątpliwości co do tożsamości rozmówcy, przekazywanie informacji zawierających dane osobowe jest zabronione.
13. Potwierdzenie prawdziwości dyplomu ukończenia studiów wyższych, jak również innych danych zawartych w dokumentach przedkładanych przez kandydata w toku rekrutacji do pracy, będącego studentem albo absolwentem Uczelni, wymaga wyraźnej zgody studenta albo absolwenta Uczelni (tzw. *background screening*).

§ 18
Monitoring poczty elektronicznej

1. Pracownik powinien wykorzystywać służbową pocztę elektroniczną (służbowy adres e- mail) jedynie do czynności związanych z wykonywaną pracą.
2. Pracownik nie powinien wykorzystywać służbowego adresu poczty elektronicznej do wysyłania prywatnej korespondencji.
3. Może być dokonywana kontrola treści służbowej korespondencji elektronicznej pracownika pod warunkiem wcześniejszego jego poinformowania. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.
4. Maile wysyłane ze służbowej poczty elektronicznej stanowią własność Uczelni.
5. W przypadku zakończenia stosunku pracy przez pracownika, Administrator Danych Osobowych może zlecić Administratorowi Systemów Informatycznych (administratorowi serwera poczty elektronicznej) przekierowanie poczty przychodzącej na inne konto poczty elektronicznej w domenie afm.edu.pl. lub uafm.edu.pl

§ 19
Przetwarzanie danych osobowych w ramach rekrutacji na studia organizowanej przez Administratora danych osobowych

1. Warunkiem ubiegania się o przyjęcie na studia, seminaria doktorskie, studia podyplomowe w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie oraz udziału w kursach, szkoleniach lub innych formach kształcenia organizowanych przez

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie jest wyrażenie przez kandydata pisemnej zgody na przetwarzanie danych osobowych.

2. Wzór formularza rekrutacyjnego wraz z oświadczeniem w przedmiocie udzielenia zgody na przetwarzanie danych osobowych zostanie opracowany każdorazowo przez radcę prawnego dla danej rekrutacji, z uwzględnieniem jej specyfiki, z rozdzieleniem celów i zakresu przetwarzania.
3. Kandydaci na studia, seminaria doktorskie oraz studia podyplomowe zapoznają się z informacjami, które Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie jako Administrator danych osobowych przekazuje im, realizując obowiązek informacyjny wynikający z art. 13 Rozporządzenia (RODO).
4. Dane osobowe kandydatów na studia oraz na studia podyplomowe przetwarzane są w systemie informatycznym „ProAkademia" obsługującym elektroniczną rejestrację na studia.
5. W przypadku odmowy przyjęcia na studia lub niepodjęcia studiów, dane osobowe umieszczone w systemie informatycznym „ProAkademia" obsługującym elektroniczną rekrutację na studia zostają usunięte, w terminie 6 miesięcy od dnia zakończenia postępowania rekrutacyjnego.
6. W przypadku zarejestrowania się w systemie obsługującym elektroniczną rejestrację na studia „ProAkademia" oraz nie przedłożenia wymaganych dokumentów, dane osobowe umieszczone w systemie informatycznym zostają usunięte, w terminie 2 miesięcy od dnia zakończenia postępowania rekrutacyjnego.

§ 20
Przetwarzanie danych osobowych studentów oraz absolwentów przez Administratora danych osobowych

1. Dane osobowe studentów, słuchaczy seminariów doktorskich, słuchaczy studiów podyplomowych, uczestników kursów oraz szkoleń przetwarzane są przez Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie w celu świadczenia usług edukacyjnych oraz w celu wypełnienia przez Uczelnię obowiązków prawnych wynikających z przepisów prawa, w szczególności z ustawy Prawo o szkolnictwie wyższym i nauce oraz aktów wykonawczych.
2. Dane osobowe studentów, studentów studiów doktoranckich, słuchaczy seminariów doktorskich, słuchaczy studiów podyplomowych, uczestników kursów oraz szkoleń przetwarzane są na papierowych nośnikach danych (dokumentacja papierowa, np. teczki akt osobowych, księgi, wykazy, listy itp.) na zasadach wynikających z przepisów prawa.
3. Dane osobowe studentów, słuchaczy studiów podyplomowych oraz absolwentów Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie przetwarzane są w wersji elektronicznej za pośrednictwem systemu informatycznego „ProAkademia".
4. System informatyczny „ProAkademia" jest aplikacją obsługującą relacyjną bazę danych. Dane dotyczące kandydatów na studia, studentów i gromadzone są w jednej bazie danych.
5. Zgodnie z relacyjnym modelem bazy danych, dane przetrzymywane są w tablicach powiązanych wzajemnie relacjami. Z punktu widzenia danych kandydatów na studia, studentów i absolwentów Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie najbardziej znacząca jest tablica o nazwie „STUD" i „OSOBA" zawierająca dane osobowe. Wykaz pól tablicy „STUD" i „OSOBA" stanowi załącznik nr 17 do Polityki Bezpieczeństwa Informacji.
6. Dane osobowe studentów wysyłane są (jednokierunkowo) z systemu „ProAkademia" do systemu „Platforma e-Learningowa". Pomiędzy tymi dwoma systemami

przekazywane są tylko następujące dane: imię i nazwisko studenta, PESEL, numer indeksu, adres e-mail, kierunek studiów, rok rozpoczęcia studiów, status studenta.
7. Dane przesyłane są do pliku o strukturze zgodnej ze standardem txt lub csv.
8. Plik z systemu „ProAkademia" wysyłany jest poprzez szyfrowane łącze protokołem ftp lub ssh poprzez określony port na komputer o określonym adresie IP. Transmisja pliku odbywa się codziennie w godzinach nocnych.
9. W systemie informatycznym „ProAkademia" stosuje się następujące środki techniczne:
   1) sieć lokalna Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie jest podłączona do sieci ogólnodostępnej Internet poprzez system firewall; na każdej stacji roboczej zainstalowany jest system antywirusowy;
   2) dostęp do komputerów, poprzez które możliwe jest logowanie się do systemu informatycznego „ProAkademia" chroniony jest przed dostępem osób trzecich poprzez hasła i loginy użytkowników na poziomie systemu operacyjnego;
   3) dostęp do systemu informatycznego „ProAkademia" posiadają wyłącznie pracownicy upoważnieni do przetwarzania danych osobowych;
   4) poziom dostępu do przetwarzanych danych osobowych w systemie informatycznym „ProAkademia" ustala Administrator systemu informatycznego w zależności od posiadanego przez użytkownika upoważnienia;
   5) użytkownik loguje się do systemu informatycznego „ProAkademia" za pomocą hasła, które posiada minimum 8 znaków i obejmuje małe oraz wielkie litery oraz cyfry lub znaki specjalne;
   6) hasło jest zmieniane nie rzadziej niż co 30 dni;
   7) hasło jest poufne i nie jest udostępniane osobom trzecim.

§ 21
Przetwarzanie danych osobowych
osób ubiegających się o zatrudnienie

1. Przetwarzanie danych osobowych osób ubiegających się o zatrudnienie w Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, innych niż wymienione w art. 22^1 § 1 i § 3 Kodeksu pracy, z wyjątkiem danych osobowych, o których mowa w art. 10 Rozporządzenia RODO, wymagają zgody osoby ubiegającej się o zatrudnienie.
2. Wzór oświadczenia w przedmiocie udzielenia zgody na przetwarzanie danych osobowych wraz z informacjami, które Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie jako Administrator danych osobowych przekazuje osobie ubiegającej się o zatrudnienie, realizując obowiązek informacyjny wynikający z art. 13 Rozporządzenia (RODO) stanowi załącznik nr 18 do Polityki Bezpieczeństwa Informacji.

§ 22
Przetwarzanie danych osobowych pracowników

1. Informacje o pracowniku, takie jak jego imię i nazwisko, służbowy: numer telefonu, adres e-mail, mogą zostać podane do publicznej informacji w obszarze Uczelni oraz na stronie internetowej bez zgody pracownika, gdyż są to dane ściśle związane z wykonywaną przez niego pracą.
2. Uczelnia przetwarza również dane finansowe pracowników oraz dotyczące ich stanu zdrowia (w szczególności zdolności do pracy), które są bezpośrednio związane ze stosunkiem zatrudnienia.
3. Administrator danych osobowych przetwarza wizerunek pracowników na podstawie odrębnie wyrażonej zgody na rozpowszechnianie lub wykorzystanie wizerunku, której

wzór zostanie opracowany każdorazowo przez radcę prawnego, z uwzględnieniem zakresu oraz celów oraz celów przetwarzania.

§ 23

Przetwarzanie danych osobowych użytkowników Biblioteki Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego

Zasady przetwarzania danych osobowych przez Bibliotekę Uniwersytetu Andrzeja Frycza Modrzewskiewskiego określa Regulamin korzystania z Biblioteki Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie.

§ 24

Przetwarzanie danych osobowych w ramach konferencji naukowych lub innych wydarzeń organizowanych przez Administratora danych osobowych

1. Dział Organizacji Konferencji Naukowych i Promocji organizując lub współorganizując konferencję naukową albo inne wydarzenie, zobowiązany jest do spełnienia obowiązku informacyjnego wynikającego z obowiązujących przepisów prawa w stosunku do osób, których dane osobowe będą przetwarzane dla celów organizacji oraz uczestnictwa w konferencji lub innego wydarzenia.
2. Wzór oświadczenia w przedmiocie udzielenia zgody na przetwarzanie danych osobowych zostanie opracowany każdorazowo przez radcę prawnego dla danego wydarzenia, z uwzględnieniem specyfiki wydarzenia, z rozdzieleniem czynności i celów przetwarzania.
3. Zamieszczanie danych w postaci wizerunku osób na stronach internetowych, w mediach społecznościowych należących do Administratora danych lub materiałach promocyjnych i folderach reklamowych Administratora danych wymaga uzyskania pisemnej zgody na przetwarzanie danych, zawierającej wyraźne oświadczenie o wyrażeniu zgody na rozpowszechnianie wizerunku, w tym jego publikację oraz przetwarzanie danych osoby, której zgoda dotyczy. Wzór zgody na rozpowszechnianie wizerunku stanowi załącznik nr 19 do Polityki Bezpieczeństwa Informacji.
4. Obowiązek pozyskania zgody na rozpowszechnianie wizerunku nie dotyczy osób powszechnie znanych w związku z pełnieniem przez nich funkcji publicznych, w szczególności politycznych, społecznych, zawodowych.
5. Obowiązek pozyskania zgody na rozpowszechnianie wizerunku nie dotyczy osoby stanowiącej jedynie szczegół całości takiej, jak zgromadzenie, krajobraz, publiczna impreza.
6. Pracownicy Administratora danych przetwarzają dane osobowe dla celów konferencji naukowej lub innego wydarzenia organizowanego przez Administratora danych wyłącznie na podstawie stosownych upoważnień do przetwarzania danych osobowych obowiązującego oraz aktów wewnętrznych.

§ 25

Środki fizyczne, techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie stosuje środki organizacyjne i techniczne, zapewniające ochronę przetwarzanych danych osobowych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.
2. Administrator danych osobowych wdraża odpowiednie środki fizyczne, techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający szacowanemu ryzyku, w tym między innymi:

Środki fizyczne:

1) przechowywanie danych osobowych w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);
2) przechowywanie danych osobowych w zamykanych na klucz szufladach, niemetalowych szafach;
3) przechowywanie danych osobowych w zamykanych na klucz w metalowych szafach, w zamkniętych sejfach lub kasach pancernych w stosownych przypadkach;
4) przetwarzanie danych osobowych w pomieszczeniach wyposażonych w system alarmowy przeciwwłamaniowy;
5) przetwarzanie danych osobowych w obszarze objętym systemem monitoringu wizyjnego z zastosowaniem kamer przemysłowych. Szczegółowe zasady dotyczące stosowania monitoringu wizyjnego w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie określa Regulamin monitoringu wizyjnego;
6) przetwarzanie danych osobowych w pomieszczeniach zabezpieczonych przed skutkami pożaru za pomocą systemu przeciwpożarowego i gaśnic;
7) dostęp do pomieszczeń, w których przechowywane są kopie zapasowe objęty systemem kontroli dostępu;
8) obszar przetwarzania danych osobowych w przypadku nieobecności pracowników nadzorowany przez służbę ochrony oraz system monitoringu wizyjnego.

Środki techniczne:

1) pseudonimizacja lub szyfrowanie danych osobowych w stosownych przypadkach, w szczególności w sytuacji, o której mowa w § 17 ust. 9 Polityki Bezpieczeństwa Informacji;
2) zabezpieczenie dostępu do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
3) stosowanie rejestracji dostępu do systemów informatycznych;
4) stosowanie środków ochrony przed szkodliwym oprogramowaniem
5) używanie systemu Firewall w celu ochrony sieci komputerowej.

Środki organizacyjne:

1) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez Administratora danych osobowych;
2) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
3) powołanie Inspektora ochrony danych osobowych;
4) wyznaczenie Administratora systemów informatycznych;
5) opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji;

6) opracowanie i wdrożenie Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych;
7) zaznajomienie osób przetwarzających dane osobowe z przepisami dotyczącymi ochrony danych osobowych;
8) zobowiązanie osób przetwarzających dane osobowe do zachowania ich w tajemnicy.

§ 26
Kontrola przetwarzania i zabezpieczenia danych osobowych

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie sprawuje Inspektor ochrony danych osobowych oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
2. Inspektor ochrony danych osobowych dokonuje czynności kontrolnych co najmniej dwa razy w roku w wybranych jednostkach organizacyjnych Uczelni oraz dokumentuje je raportami przedkładanymi Administratorowi danych osobowych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami Rozporządzenia (RODO).

§ 27
Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Inspektorowi ochrony danych osobowych lub Administratorowi systemów informatycznych (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Jednocześnie osoba powiadamiająca powinna:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   2) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   3) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, Inspektor ochrony danych osobowych lub Administrator systemów informatycznych:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania;
   2) wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
4. Inspektor ochrony danych osobowych lub Administrator systemów informatycznych dokumentuje zaistniały przypadek naruszenia sporządzając raport, którego wzór stanowi załącznik nr 20 do Polityki Bezpieczeństwa Informacji.
5. Inspektor ochrony danych osobowych lub Administrator Systemów Informatycznych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze wydając zalecenia (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

6. W przypadku naruszenia ochrony danych osobowych skutkującego wysokim ryzykiem naruszenia prac lub wolności osób, Inspektor ochrony danych osobowych lub Administrator systemów informatycznych dokonuje zgłoszenia naruszenia do Organu nadzorczego w terminie 72 godzin.
7. W przypadku incydentu w zakresie ochrony danych osobowych, który nie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób, Inspektor ochrony danych osobowych wydaje zalecenia i odnotowuje zaistniały incydent w prowadzonym Rejestrze incydentów.
8. Do zdarzeń mogących prowadzić do naruszenia ochrony danych osobowych zalicza się między innymi:
   1) kradzież danych w każdej formie,
   2) nieumyślną lub celową modyfikację danych, zarówno w formie elektronicznej i papierowej,
   3) utratę danych,
   4) włamania do systemu poprzez programy, takie jak wirus, koń trojański, makro, bomba logiczna,
   5) awarie sprzętu lub uszkodzenie oprogramowania,
   6) utratę zasilania powodującą przerwę w pracy systemów,
   7) zabór sprzętu lub nośników z ważnymi danymi,
   8) nieprzestrzeganie postanowień Polityki,
   9) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych, zjawiska takie jak: naturalne katastrofy, działania silnych pól elektromagnetycznych, przechwycenie transmisji danych.

§ 28
Zarządzanie ryzykiem

1. Każde zidentyfikowane ryzyko podlega analizie w zakresie jego wpływu na bezpieczeństwo informacji oraz prawdopodobieństwa wystąpienia tego ryzyka. Wykaz typowych zagrożeń (ryzyk) dla bezpieczeństwa danych osobowych stanowi załącznik nr 21 do Polityki Bezpieczeństwa Informacji.
2. Ustala się trzystopniową skalę oceny wpływu ryzyka na bezpieczeństwo informacji oraz trzystopniową miarę prawdopodobieństwa wystąpienia ryzyka. Miara istotności ryzyka bierze pod uwagę obydwa te czynniki, to jest miarę wpływu ryzyka oraz miarę prawdopodobieństwa wystąpienia ryzyka. Ustala się ją jako iloczyn tych dwu miar.
3. Podczas oceny wpływu ryzyka i prawdopodobieństwa jego wystąpienia należy wziąć pod uwagę klasyfikację informacji na które wpływ może mieć zidentyfikowane ryzyko. Poniżej zdefiniowano miarę wpływu ryzyka, miarę prawdopodobieństwa jego wystąpienia oraz miarę istotności ryzyka:
4. Miara wpływu ryzyka na bezpieczeństwo informacji:
   1) W1 (niski, 2 punkty) – zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, zakłócenie lub opóźnienie w wykonywaniu zadań; nie wpływa na reputację; skutki zdarzenia można łatwo usunąć;
   2) W2 (średni, 4 punkty) – zdarzenie objęte ryzykiem powoduje znaczną stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację; z wystąpieniem zdarzenia może wiązać się trudny proces przywracania stanu poprzedniego;
   3) W3 (duży, 6 punktów) – zdarzenie objęte ryzykiem powoduje uszczerbek mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań albo osiągania

założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa lub na reputacji.

5. Miara wpływu ryzyka związanego z aktywami informacyjnymi wyznaczana jest na podstawie klasyfikacji danych aktywów informacyjnych. Należy przyjąć, że dla aktywów informacyjnych, których klasyfikacje są na poziomie niskim **(C1, I1, A1)** miara wpływu ryzyka wynosi W1. Dla ryzyka związanego z aktywami informacyjnymi dla których, dowolna z klasyfikacji jest na poziomie średnim (C2, I2, A2) miara wpływu ryzyka wynosi W2. Dla ryzyka związanego z aktywami informacyjnymi dla których, dowolna z klasyfikacji jest na poziomie wysokim (C3, I3, A3) miara wpływu ryzyka wynosi W3.
6. Miara prawdopodobieństwa wystąpienia ryzyka:

   1) P1 (niskie, 2 punkty) – istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz w ciąg roku lub nie zdarzy się wcale (w ciągu roku);
   2) P2 (średnie, 4 punkty) – istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku;
   3) P3 (duże, 6 punktów) – istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku.
7. Miara istotności ryzyka:

   1) IR1 (niska) – iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 4 do 8 punktów;
   2) IR2 (średnia) – iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 12 do 16 punktów;
   3) IR3 (duża) – iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 24 do 36 punktów.
8. W zależności od zidentyfikowanego poziomu ryzyka określa się zasady postępowania z ryzykiem:

   1) ryzyko o niskiej istotności należy traktować jako akceptowalne. Zaakceptowanie ryzyka nie wyklucza możliwości jego monitorowania oraz podejmowania działań zaradczych;
   2) ryzyko oznaczone jako średnie wymaga rozważenia potrzeby wdrożenia działań zaradczych. W sytuacji, gdy zostanie podjęta decyzja o tolerowaniu ryzyka oznaczonego jako średnie, dokonać powtórnej oceny istotności ryzyka nie później niż po 6 miesiącach od daty decyzji o tolerowaniu ryzyka. W sytuacji gdy poziom istotności dla takiego ryzyka nie ulegnie zmianie, postępujemy tak, jak w przypadku ryzyka o wysokim poziomie istotności;
   3) ryzyko oznaczone jako duże wymaga wprowadzenia działań zaradczych (reakcji na ryzyko), w tym modyfikacji lub uzupełnienia mechanizmów kontroli, które ograniczają możliwości wystąpienia ryzyka;
   4) decyzję o akceptacji dużego ryzyka może podjąć Rektor.
9. Ustala się następujące sposoby ograniczania ryzyka:

   1) przeniesienie ryzyka (np. ubezpieczenie);
   2) akceptację ryzyka (trudności w przeciwdziałaniu lub gdy koszty podjętych działań mogą przekroczyć przewidywane korzyści);
   3) przeciwdziałanie (np. wzmocnienie mechanizmów kontrolnych, podjęcie działań zmniejszających prawdopodobieństwo wystąpienia niepożądanych sytuacji);
   4) przesunięcie w czasie (np. wycofanie się z realizacji zadania, gdy jego realizacja wiąże się z pojawieniem się dużego ryzyka).

10. Proces zarządzania ryzykiem związanym z bezpieczeństwem informacji musi zostać udokumentowany w postaci dokumentu w postaci tradycyjnej (papierowej) lub elektronicznej, który zawiera:
    1) obszar ryzyka;
    2) jednoznaczne określenie ryzyka;
    3) zidentyfikowane podatności;
    4) działania ograniczające ryzyko z określeniem terminów realizacji tych działań i osób odpowiedzialnych.
11. Akceptacja Ryzyka wymaga sporządzenia Dokumentu Akceptacji Ryzyka zawierającego co najmniej:
    1) opis ryzyka;
    2) klasyfikację istotności ryzyka;
    3) opis stanu dotychczasowego;
    4) zastosowane środki ograniczające ryzyko;
    5) końcową ocenę poziomu ryzyka (niskie, średnie lub duże);
    6) datę ważności akceptacji (dopuszcza się ważność bezterminową dla ryzyka ocenionego jako niskie).
12. Dokumentu Akceptacji Ryzyka w przypadku akceptacji zidentyfikowanych ryzyk o istotności średniej lub dużej średniej dokonuje Rektor lub inna osoba upoważniona.

Wykaz załączników do Polityki Bezpieczeństwa Informacji Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie:

1) Wzór Rejestru czynności przetwarzania danych osobowych;
2) Wzór Rejestru kategorii przetwarzania danych osobowych;
3) Wzór Rejestru umów powierzenia przetwarzania danych osobowych;
4) Wzór Rejestru udostępnień danych osobowych;
5) Wzór Rejestru incydentów dotyczących ochrony danych osobowych;
6) Spis systemów informatycznych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie;
7) Wzór upoważnienia do przetwarzania danych osobowych wraz ze wzorem oświadczenia osoby upoważnianej do zachowania tajemnicy;
8) Wzór ewidencji upoważnień do przetwarzania danych osobowych;
9) Wzory przykładowej klauzuli informacyjnej (informacji dotyczących przetwarzania danych osobowych);
10) Wzór informacji o danych osobowych przetwarzanych przez Administratora danych osobowych;
11) Wzór umowy powierzenia przetwarzania danych osobowych;
12) Wykaz budynków, pomieszczeń oraz części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe;
13) Instrukcja korzystania z urządzeń informatycznych, w szczególności komputerów, drukarek oraz oprogramowania komputerowego, a także wewnętrznej sieci komputerowej w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie;
14) Instrukcja Zarządzania Systemami Informatycznymi w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie;
15) Zasady tzw. „czystego biurka” oraz „czystego ekranu” w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie;

16) Wzór zgody na przetwarzanie i udostępnienie prywatnego adresu e-mail przez pracowników wykonujących obowiązki dydaktyczne wraz z klauzulą informacyjną;
17) Wykaz pól tablicy „STUD" i „OSOBA" w systemie ProAkademia;
18) Wzór zgody na przetwarzanie danych osobowych na potrzeby rekrutacji do pracy wraz z klauzulą informacyjną;
19) Wzór zgody na przetwarzanie wizerunku w ramach konferencji naukowych lub innych wydarzeń organizowanych lub współorganizowanych przez Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie;
20) Wzór raportu naruszenia ochrony danych osobowych;
21) Wykaz typowych zagrożeń (ryzyk) dla ochrony danych osobowych.

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji

Rejestr Czynności przetwarzania danych osobowych
UNIWERSYTETU ANDRZEJA FRYCZA MODRZEWSKIEGO

Lp.	Nazwa czynności przetwarzania	Jednostka organizacyjna - Odpowiedzialny za działanie	Kategorie osób - (dane osobowe wejściowe - jakie osoby - rodzaj) art. 30 ust. 1 pkt c RODO	Kategorie (zakres) danych osobowych (dane osobowe wejściowe) - art. 30 ust. 1 pkt C RODO	dane osobowe przekazane papierowo/elektorniczne/ wizja/głos	wsparcie IT - (wewnętrzne, czy zewnętrzne) - nazwa systemu lub oprogramowania	Źródło danych osobowych (od kogo uzyskane dane z jakiego źródła)	Podstawa prawna przetwarzania(zgoda/postępowanie przed umową/umowa/inna podstawa przetwarzania)	Kategorie odbiorców (innych niż podmiot przetwarzający; przekazne do kogo ? ODBIORCY - art. 30 ust.1 pkt d RODO	czy to osoba/ podmiot uprawniony ? - podstawa uprawnienia ? (powierzenie , upoważnienie, z mocy prawa)

Cel przetwarzania danych - art. 30 ust. 1 pkt b RODO	Termin/okres przetwarzania danych do osiągnięica rezultatu - art. 30 ust. 1 pkt f RODO (jeśli jest to możliwe)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 RODO (jeśli jest to możliwe) - art. 30 ust 1 pkt g RODO	Transfer do kraju trzeciego lub org. Międzynarodowej - (nazwa kraju i podmiotu; dokumentacja) art. 30 ust. 1 pkt e RODO

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji

Rejestr kategorii czynności przetwarzania w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie

Lp.	Kategorie przetwarzań (art. 30 ust. 2 lit. b RODO)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeśli jest to możliwe) art. art. 30 ust. 2 lit. d, art. 32 ust. 1 RODO)	Administrator (Art. 30 ust. 2 lit. a RODO) a) Nazwa i dane kontaktowe administratora; b) Nazwa i dane kontaktowe współadministratora; c) Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono) d) Inspektor ochrony danych administratora	Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane (Art. 30 ust. 2 lit. c RODO)	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi (Art. 30 ust. 2 lit. c RODO)	Podprzetwarzający (podwykonawca) - jeśli dotyczy Nazwa i dane kontaktowe podprzetwarzającego; Kategorie podpowierzonych przetwarzań

Załącznik nr 3 do Polityki Bezpieczeństwa Informacji

REJESTR UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Dane identyfikacyjne Podmiotu Przetwarzającego	Zakres umowy	Data zawarcia umowy/aneksu	Okres obowiązywania umowy	Miejsce przechowania umowy w wersji papierowej

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji

REJESTR UDOSTĘPNIEŃ DANYCH OSOBOWYCH

Lp.	Podmiot, któremu dane udostępniono	Nazwa zbioru, z którego udostępniono dane	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych	Data udostępnienia/udzielenia odpowiedzi	Imię i nazwisko pracownika dokonującego udostępnienia

Załącznik nr 5 do Polityki Bezpieczeństwa Informacji

REJESTR ZDARZEŃ (INCYDENTÓW)
UNIWERSYTETU ANDRZEJA FRYCZA MODRZEWSKIEGO W KRAKOWIE

Lp.	Data zdarzenia	Opis zdarzenia	Jednostka/osoba/miejsce/działanie IODO	Zalecenia

Załącznik nr 6 do Polityki Bezpieczeństwa Informacji

Wykaz systemów informatycznych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie

1.System ProAkademia (APR)

2. System SAGE Symfonia ERP (4 moduły tj. * Handel, Kadry i Płace, Finanse i Księgowość, Środki Trwałe)

2a.) Repozytorium dokumentów Kadry i Płace, Repozytorium dokumentów ERP, repozytorium dokumentów Administrator

3. System Płatnik

4. System Elektronicznej Legitymacji Studenckiej

5. System Elektronicznej Legitymacji Doktoranckiej

6. System Portiernia

7. Serwis elektronicznej rejestracji kandydatów na studia

8. Serwis elektronicznej rejestracji kandydatów na studia podyplomowe

9. System Pol-on

10. System E-learning

11. System Syllabus

12. System Dorobek Naukowy

13. Systemy Antyplagiatowe: Otwarty System Antyplagiatowy i Jednolity System Antyplagiatowy

14. System Biblioteczny

15. Repozytorium Zbiorów Erika

16. System Microsoft 365

17. System Microsoft Imagine

18. Systemy elektronicznych baz danych: EBSCO, ClinicalKey, EMIS, SpringerLink, Web of Science

19. System CSL (Centralny System Logowania)

20. System EOD (Elektroniczny Obieg Dokumentów)

21. System Multiportal

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119) – dalej zwanego RODO

upoważniam
Panią/Pana……
(imię i nazwisko)

Zatrudnionego/ą w

……

(*pełna nazwa wydziału/jednostki)*

na podstawie: umowy o pracę/umowy zlecenia/umowy o dzieło*

do przetwarzania danych osobowych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie w ramach powierzonych obowiązków służbowych, w zakresie niezbędnym do ich realizacji, w następujących zbiorach danych osobowych **:

1.	kandydatów na studia	
2.	studentów	
3.	absolwentów	
4.	kandydatów do pracy	
5.	pracowników	
6.	byłych pracowników	
7.	stażystów	
8.	byłych stażystów	
9.	wykonawców z umów cywilnoprawnych	
10.	Inne:	

i następujących systemach informatycznych Uczelni ** :

1.	System ProAkademia (APR)	
2.	Systemu Finansowo - Księgowy - SAGE Symfonia	
3.	System Płatnik	
4.	System Elektronicznej Legitymacji Studenckiej	
5.	System Portiernia	
6.	Serwis elektronicznej rejestracji kandydatów na studia	
7.	Serwis elektronicznej rejestracji kandydatów na studia podyplomowe	
8.	System Pol-on	
9.	System E–learning	

10.	System Syllabus	
11.	System Dorobek Naukowy	
12.	Systemy Antyplagiatowe: (Jednolity System Antyplagiatowy)	
13.	System biblioteczny	
14.	System CSL (Centralny System Logowania)	
15.	System EOD (elektroniczny obieg dokumentów)	
16.	System Multiportal	

Inne programy komputerowe**:

1.	Aplikacje biurowe (Word, Excel)	
2.	Program do sprawdzania prac zaliczeniowych	
3.	Inne:	

1. Informuję, że przetwarzanie danych osobowych musi być zgodne z udzielonym upoważnieniem, przepisami RODO, ustawą o ochronie danych osobowych, innymi przepisami prawa oraz wewnętrznymi regulacjami w sprawie ochrony danych osobowych.
2. Może Pani/Pan, w ramach wykonywanych obowiązków i zgodnie z obowiązującymi przepisami prawa przetwarzać dane osobowe z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Krakowskiej Akademii.
3. Zobowiązuję Panią/Pana do zachowania przetwarzanych danych w tajemnicy.
4. Informuję, że przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności karnej, o której mowa w ustawie o ochronie danych osobowych.
5. Upoważnienie traci moc z dniem odwołania niniejszego upoważnienia, zmiany zajmowanego stanowiska, ustania stosunku pracy lub wygaśnięcia innego zobowiązania na podstawie, którego osoba otrzymała niniejsze upoważnienie.

.....

Pieczęć i podpis osoby reprezentującej
Administratora Danych

Zobowiązuję się do przetwarzania danych jedynie zgodnie z udzielonym upoważnieniem, przepisami RODO, ustawą o ochronie danych osobowych, innymi przepisami prawa oraz wewnętrznymi regulacjami w sprawie ochrony danych osobowych, a także do zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po wygaśnięciu upoważnienia

.....

Czytelny podpis osoby upoważnionej

Załącznik nr 8 do Polityki Bezpieczeństwa Informacji

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

nr skier.	numer upoważnienia	nazwisko imię	Jednostka organizacyjna	forma umowy	data otrzymania upoważnienia	data wygaśnięcia

Załącznik nr 9 do Polityki Bezpieczeństwa

Zgodnie z art. 13 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 (…) („RODO") Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie informuje, iż:

1. Administratorem Pani/Pana danych osobowych jest Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie, ul. Gustawa Herlinga Grudzińskiego 1, 30-705 Kraków.
2. Uczelnia powołała Inspektora Ochrony Danych Osobowych, z którym może się Pani/Pan skontaktować w przypadku jakichkolwiek pytań lub uwag dotyczących przetwarzania Pani/Pana danych osobowych, przy ul. Gustawa Herlinga-Grudzińskiego 1 w Krakowie lub za pośrednictwem adresu e-mail: iodo@afm.edu.pl.
3. Pani/Pana dane osobowe będą przetwarzane w celu ……...
4. Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. ……, art. 9…….. RODO.
5. Podanie przez Panią/Pana danych osobowych jest dobrowolne, lecz odmowa ich podania jest równoznaczna z brakiem możliwości …… (*w przypadku przetwarzania danych osobowych na podstawie zgody*). Odbiorcami Pana/Pani danych osobowych mogą być podmioty ……...
6. Pani/Pana dane osobowe będą przechowywane przez czas trwania …….. oraz czas niezbędny do ewentualnych postępowań wyjaśniających/dochodzenia roszczeń ……. oraz okres archiwizacji wynikający z przepisów prawa.
7. Dane osobowe mogą zostać udostępnione innym podmiotom wyłącznie posiadającym odpowiednie upoważnienie na podstawie przepisów prawa krajowego lub unijnego.
8. Posiada Pani/Pan prawo dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; wycofanie zgody na przetwarzanie danych osobowych można przesłać e-mailem na adres: iodo@afm.edu.pl lub pocztą tradycyjną na adres: ul. Gustawa Herlinga Grudzińskiego 1, 30-705 Kraków.
9. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.
10. Udostępnione dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddane profilowaniu oraz nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

……

data i czytelny podpis

Załącznik nr 10 do Polityki Bezpieczeństwa Informacji

Kraków, dnia.....

Pani/Pan
Imię i Nazwisko
Adres

Informacja o danych osobowych

W związku z Pani/ Pana* wnioskiem z dnia ..... o udzielenie informacji związanych z przetwarzaniem danych osobowych przez Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie, działając na podstawie art. 15 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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, zwanego dalej „Rozporządzenie RODO", uprzejmie informuję, że Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie przetwarza następujące dane osobowe dotyczące Pani/ Pana*:

1. imiona: .....
2. nazwisko: .....
3. data urodzenia: .....
4. adres zamieszkania/ do korespondencji: .....
5. nr ewidencyjny **PESEL/nr albumu**: .....
6. seria i nr dowodu osobistego: .....
7. inne dane (podać jakie): .....

Powyższe dane są przetwarzane w ……. (podać nazwę jednostki) w celu ..... z zachowaniem wymaganych zabezpieczeń i zostały uzyskane:

- bezpośrednio od Pani/ Pana*.....
- w inny sposób (podać jaki).....

Powyższe dane nie były / były* udostępniane (podać komu) ……..... w celu.....

Zgodnie z art. 15-22 Rozporządzenia RODO przysługują Pani/ Panu* prawo do uzyskania dostępu do dotyczących Pani/Pana danych osobowych, prawo do sprostowania danych, prawo do usunięcia danych, prawo do ograniczenia przetwarzania danych osobowych.

Z upoważnienia Administratora Danych Osobowych

……

* niepotrzebne skreślić

Załącznik nr 11 do Polityki Bezpieczeństwa Informacji

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia _____ pomiędzy:
(zwana dalej „Umową")

_____ *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Podmiotem przetwarzającym"**
reprezentowana przez:
_____

oraz

_____ *(*dane podmiotu który umowę zawiera)*

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

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (**należy podać rodzaj danych*) …… *np. dane zwykłe oraz dane szczególnych kategorii ……. (*należy podać kategorię osób, których dane dotyczą*) *np. pracowników administratora, klientów administratora itd. w postaci …….. np. imion i nazwisk, adresu zamieszkania, nr PESEL itd*.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu …….. (**należy podać cel przetwarzania danych przez podmiot przetwarzający*) *np. realizacji umowy z dnia …… nr …… w zakresie prowadzenia kadr.*

§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. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. 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.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 godzin.

§4

Prawo kontroli

1. Administrator danych 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 danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum …….. *(*należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).
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 może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.

4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 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 jej zawarcia przez czas *nieokreślony/określony* od ..... do ..... .*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem …… * okresu wypowiedzenia.

§8

Rozwiązanie umowy

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

§9

Zasady zachowania poufności

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

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.

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 danych.

_____	_____
Administrator danych	Podmiot przetwarzający

Załącznik nr 12 do Polityki Bezpieczeństwa Informacji

Wykaz budynków, pomieszczeń oraz części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe

Budynki przy ul. G. Herlinga - Grudzińskiego 1, 30-705 Kraków

1) Budynek A

PODZIEMIE

Nr. pom.	Nazwa pomieszczenia
-119, -125	Archiwum

PARTER

Nr. pom.	Nazwa pomieszczenia
003	Portiernia + Centrala pożarowa bud A, B i C
	Kasa
003b	Pomieszczenie Ochrony
009	Pokój Prodziekanów Wydziału Zarządzania i Komunikacji Społecznej
010	Biuro Zarządzania Projektami
011	Pracownia Projektowania Przestrzennego i 3D
013	Samorząd Studentów, Studencka Poradnia Prawna
014	Pracownia Psychologii
043	Pokój Lektorów

PIĘTRO I

Nr. pom.	Nazwa pomieszczenia
111, 112, 115	Dziekanat Wydziału Zarządzania i Komunikacji Społecznej
116	Pokój Dziekana Wydziału Zarządzania i Komunikacji Społecznej
117,118	Studium Języków Obcych
136	Serwerownia

PIĘTRO II

Nr. pom.	Nazwa pomieszczenia
203	Pokój Wykładowców
209,210	Dziekanat Wydziału Psychologii, Pedagogiki i Nauk Humanistycznych
211	Pokój Prodziekana Wydziału Psychologii, Pedagogiki i Nauk Humanistycznych

212	Pokój Dziekana i Prodziekana Wydziału Psychologii, Pedagogiki i Nauk Humanistycznych
213	Dział Automatyków
213a	Serwerownia
215, 216, 219	Dział Nauczania
216	Dział Nauczania
218	Oficyna Wydawnicza
228	Pokój Techników CSM

2) Budynek B

PODZIEMIE

Nr. pom.	**Nazwa pomieszczenia**
-117, -118	Studium Wychowania Fizycznego i Sportu / AZS

PARTER

Nr pom.	**Nazwa pomieszczenia**
003	Biuro Karier
004	Portiernia - zaplecze
013	Dział Organizacji Konferencji Naukowych i Promocji
014	Dział Organizacyjno-Prawny i Spraw Studenckich

PIĘTRO I

Nr pom.	**Nazwa pomieszczenia**
103	**Dział Spraw Osobowych; Radca prawny**
104, 104a	Studium Informatyki i Centrum E-learningu
108, 109	Dział Informatyki: Pokój Informatyków, Magazyn Informatyków
109a	Serwerownia
120	Oficyna Wydawnicza/KTE
121,121a, 122	Dział Spraw Osobowych

PIĘTRO II

Nr pom.	**Nazwa pomieszczenia**
205	Dział Współpracy Międzynarodowej
210	Katedra Wydziału Psychologii
211, 212	Sekretariat oraz Gabinet Prorektora ds. studenckich
213,214	Gabinet Prorektora ds. ogólnych
215	Radca prawny
216	Gabinet Rektora Prorektora ds. nauki i nauczania
221	Rektorat – Sekretariat

3) Budynek C

PODZIEMIE

Nr pom.	Nazwa pomieszczenia
-108	**Magazyn Biblioteki**
-110	Archiwum Działu Spraw Finansowych
-124	Dział Rekrutacji (Centrum Personalizacji)
-126	Serwerownia

PARTER

Nr pom.	Nazwa pomieszczenia
004	Portiernia
014,017	Dziekanat Wydziału Nauk o Zdrowiu
019,020, 021,022	Dział Spraw Finansowych
048	Hol Działu Rekrutacji
049, 051, 055, 056	Dział Rekrutacji
hol	Portiernia Pokoi Gościnnych
053	Biuro ds. Osób Niepełnosprawnych
054	Kierownik Obiektu Uczelni

PIĘTRO I

Nr pom.	Nazwa pomieszczenia
106, 107, 109-118	Biblioteka

PIĘTRO II

Nr pom.	Nazwa pomieszczenia
208E, 208F	Studio filmowo-telewizyjne
219	Centrum Studiów Podyplomowych, Seminaria doktorskie
222, 224	Dziekanat Wydziału Prawa, Administracji i Stosunków Międzynarodowych
225	Pokój Dziekana i Prodziekanów Wydziału Prawa, Administracji i Stosunków Międzynarodowych
232	Serwerownia

PIĘTRO III

Nr pom.	Nazwa pomieszczenia
311	Dział Badań Naukowych i Rozwoju
330	Pokój Dziekana Wydziału Nauk o Bezpieczeństwie
330a	Pokój Prodziekanów Wydziału Nauk o Bezpieczeństwie
332	Dziekanat Wydziału Nauk o Bezpieczeństwie
333a	Pokój Rzecznika Praw Akademickich

4) **Budynek D**

PARTER

Nr pom.	Nazwa pomieszczenia
	Portiernia
008	Centrum Doskonałości Dydaktycznej

PIĘTRO I

Nr pom.	Nazwa pomieszczenia
112	Serwerownia
115	Pokój Dziekanów Wydziału Lekarskiego
116	Sekretariat
117	Pokój Prorektora ds. Collegium Medicum
118	Pokój Dziekanów Wydziału Nauk o Zdrowiu
119	Dziekanat kierunku lekarskiego
120	Administracja kierunku lekarskiego

PIĘTRO II

Nr pom.	Nazwa pomieszczenia
221	Pokój Dziekanów Wydziału Architektury i Sztuk Pięknych oraz Pokój Dziekanów Wydziału Aktorskiego
222	Dziekanat Wydziału Architektury i Sztuk Pięknych oraz Dziekanat Wydziału Aktorskiego

Załącznik nr 13 do Polityki Bezpieczeństwa Informacji

Instrukcja korzystania z urządzeń informatycznych, w szczególności komputerów, drukarek oraz oprogramowania komputerowego, a także wewnętrznej sieci komputerowej w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie

§ 1

Zasady ogólne korzystania z urządzeń informatycznych oraz wewnętrznej sieci komputerowej:

1. Wszystkie urządzenia komputerowe, oprogramowanie oraz drukarki dopuszczone do użytku w sieci Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie dostarcza Dział IT.
2. Sprzęt komputerowy zainstalowany w przeznaczonym do tego celu miejscu nie może być przenoszony w inne miejsce bez wiedzy i zgody Działu IT, za wyjątkiem komputerów przenośnych.
3. Podłączenie innych urządzeń do sieci komputerowej wymaga uzyskania uprzedniej zgody Działu IT.
4. Samowolne instalowanie, kopiowanie i używanie jakiegokolwiek oprogramowania, niż zainstalowane przez pracowników Działu IT, na komputerach jest zabronione.
5. W uzasadnionych przypadkach Dział IT może wyrazić zgodę na instalowanie dodatkowego oprogramowania przez pracownika.
6. Podłączanie komputerów oraz innych urządzeń do innych sieci w jakikolwiek sposób jest zabronione.
7. Użytkownikom nie wolno tworzyć kopii licencjonowanego oprogramowania oraz kopii plików konfiguracyjnych systemu operacyjnego.
8. Użytkownikom nie wolno celowo podejmować akcji mających znamiona:
    1. nękania innych użytkowników,
    2. obniżania wydajności urządzeń komputerowych,
    3. pozbawiania uprawnionych użytkowników dostępu do zasobów,
    4. obchodzenia zabezpieczeń w celu uzyskania nieuprawnionego dostępu do zasobów,
    5. przestępstwa lub wykroczenia.
9. Użytkownikom nie wolno uzyskiwać dostępu do danych i aplikacji, do których użycia nie mają uprawnień.
10. Wobec pracowników naruszających powyższe zasady Pracodawca może zastosować środki odpowiedzialności porządkowej, a w sytuacji rażącego ich naruszenia, rozwiązać umowę o pracę bez wypowiedzenia z winy pracownika (art. 52 § 1 pkt 1).
11. W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu systemu, użytkownik powinien poinformować Dział IT.

§ 2

Zasady korzystania z urządzeń informatycznych – sprzętu komputerowego:

1. Sprzęt komputerowy Zintegrowany jest z infrastrukturą teleinformatyczną Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie. Dotyczy to konfiguracji sieci, standardowych aplikacji biurowych oraz uwierzytelnienia użytkownika.
2. Rozpoczęcie pracy możliwe jest wyłącznie po podaniu nazwy użytkownika oraz hasła.

3. W uzasadnionych przypadkach Dział IT może ustanawiać dodatkowe metody autoryzacji i uwierzytelnienia użytkownika.
4. Każda stacja robocza wyposażona jest w zestaw standardowego oprogramowania niezbędnego do pracy.
5. Stacje robocze wyposażone są w twarde dyski, z prawem zapisu przez użytkownika danych. Dane przechowywane na dyskach lokalnych komputerów nie są chronione przed nieautoryzowanym dostępem ani archiwizowane. Istnieje zatem możliwość utraty danych w wypadku awarii sprzętu lub skasowania przez innego użytkownika na dyskach lokalnych.
6. Zabronione jest przechowywanie informacji oznaczonych klauzulą tajne lub poufne na dyskach lokalnych.
7. Użytkownik posiada własny dysk sieciowy U:, na którym może przechowywać dane. Zasoby te są chronione przed nieautoryzowanym dostępem i archiwizowane.
8. Użytkownik sieci ma również dostęp do dysku sieciowego W:, w którym znajdują się foldery z określonymi prawami dostępu oraz odpowiadające poszczególnym grupom roboczym w sieci. Foldery te służą do wymiany danych pomiędzy użytkownikami w ramach danej grupy roboczej.
9. W całej sieci komputerowej oraz na dyskach sieciowych mogą być stosowane mechanizmy blokady określonych formatów plików.
10. Zalecane jest wykorzystywanie dysków sieciowych (dysk W:.) w celu udostępniania plików określonym użytkownikom. Struktura folderów i dostępu użytkowników na dyskach sieciowych dostosowane są potrzeb Uczelni. Dodatkowe elementy dodawane są przez Dział IT na wniosek pisemny (email) kierowników działów.
11. Dane przechowywane na dyskach sieciowych podlegają archiwizacji.
12. Wszystkie komputery są konfigurowane przez Dział IT.
13. Użytkownicy nie mają praw zmiany konfiguracji sprzętu.
14. W komputerach może występować blokada stosowania zewnętrznych pamięci masowych. O możliwości usunięcia wymienionej blokady decyduje Dział IT.
15. Przenośne pamięci masowe przed dopuszczeniem do użytkowania muszą zostać zaszyfrowane przez Dział IT.
16. Nieautoryzowane oprogramowanie będzie niezwłocznie kasowane z jednoczesnym sprawdzeniem źródła pochodzenia. Wszystkie media (CD, pendrive itp.) przed wykorzystaniem powinny być sprawdzane udostępnionym przez Dział IT programem antywirusowym

§ 3

Zasady logowania do sieci komputerowej – systemu:

Ustala się następujące zasady logowania do systemu:

1. Każdy pracownik Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie otrzymuje login identyfikujący użytkownika w sieci. Standardowy login złożony jest z pierwszej litery imienia oraz nazwiska. W uzasadnionych przypadkach Dział IT może przypisać inną nazwę użytkownika.
2. Unikalna nazwa użytkownika wykorzystywana jest przy dostępie do sieci, w systemie poczty elektronicznej oraz przy logowaniu się przez Centralny System Logowania.
3. Pracownicy ponoszą odpowiedzialność za działania wykonane z użyciem ich

identyfikatora. Zabronione jest zezwalanie na korzystanie z loginu przez osoby trzecie.
4. Osoba, która uzyskuje nieautoryzowany dostęp do urządzeń komputerowych może zostać pociągnięta do odpowiedzialności karnej, a także cywilnej.
5. Bezpieczeństwo dostępu do systemu oraz danych przechowywanych na koncie użytkownika zapewnia hasło, a w przypadku Systemu Centralnego Logowania metoda 2FA.

§ 4

Zasady chronienia hasła dostępu do systemu:

1. Długość hasła nie może być mniejsza niż 8 (osiem) znaków.
2. Hasło powinno być zmieniane co najmniej raz na 30 dni (nie dotyczy systemów objętych metodą 2FA).
3. Hasła użytkowników muszą być „silne". Dla bezpieczeństwa nie powinno stosować się w hasłach informacji osobistych takich jak imiona, daty, numery dokumentów itp.
4. Użytkownik nie może konstruować haseł w znaczący sposób podobnych do wcześniej używanych. Hasło nie może powtarzać się przez kolejne 24 cykle.
5. Hasła nie mogą być ujawniane przez użytkowników. Zakaz dotyczy również ujawniania haseł administratorom, przełożonym oraz innym pracownikom.
6. Hasło musi zostać zmienione w przypadku podejrzenia jego ujawnienia osobie nieupoważnionej,
7. Użytkownik, który zapomniał hasła musi skontaktować się z Działem IT w celu wykonania procedury resetu hasła. W takim przypadku administrator wprowadzi hasło startowe i poda go użytkownikowi. Po zalogowaniu użytkownik musi je zmienić na własne.
8. W przypadku poświadczeń pozwalających na logowanie przez Centralny System Logowania użytkownik może zresetować hasło samodzielnie. Link pozwalający na resetowanie hasła wysyłany jest na prywatny adres e-mail znajdujący się w kartotece pracownika.
9. Hasła powinny być przetrzymywane w sposób niepozwalający na dostęp osobom postronnym i nieupoważnionym.

§ 5

Zasady korzystania z Internetu oraz poczty elektronicznej:

1. Możliwość korzystania z Internetu i poczty elektronicznej ma służyć wspomaganiu efektywności wykonywanej pracy.
2. Niedozwolone jest wykorzystywanie tych mediów do celów niezgodnych z prawem.
3. Pracownikom Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie nadawane są adresy email w domenach: afm.edu.pl, uafm.edu.pl.
4. Pracownik jest osobiście odpowiedzialny za informację wysyłane do użytkowników Internetu przy użyciu przydzielonego mu identyfikatora.
5. Niedozwolone jest wykorzystanie zasobów komputerowych i łącza Internet do wszelkich czynności mogących prowadzić do dostępu do informacji o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo.
6. Wszystkie dokumenty zawierające dane osobowe przed wysłaniem pocztą elektroniczną powinny zostać zaszyfrowane
7. Rozmiar skrzynki pocztowej ustalany jest indywidualnie dla użytkownika.

8. Pocztę email użytkownicy muszą traktować jako medium niezabezpieczone.
9. Poczta email nie gwarantuje czasu oraz skuteczności dostarczenia informacji.
10. W przypadku dostępu do poczty email za pomocą urządzeń mobilnych (laptopy, smartfony, tablety itp.) urządzenia te powinny być zabezpieczone w sposób niepozwalający na dostęp osobom postronnym i nieupoważnionym.

§ 6

Zasady pozostawiania użytkowanych komputerów oraz korzystania z komputerów innych użytkowników:

1. Nie należy pozostawiać zalogowanego do sieci komputera osobistego bez nadzoru. W każdym przypadku pozostawienia komputera bez osobistego nadzory należy się wylogować lub zablokować komputer.
2. Nie powinno się używać komputerów, na których jest zalogowany inny użytkownik. Jeśli z okoliczności wynika, że użytkownik danego komputera nie będzie już na nim pracował, należy wykonać operację przelogowania się na swój identyfikator.
3. Użytkownik powinien stosować politykę tzw. „czystego biurka”.

Załącznik nr 14 do Polityki Bezpieczeństwa Informacji

Instrukcja zarządzania systemem informatycznym Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie

Wprowadzenie

Niniejsza **INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM** stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z art. 32 Rozporządzenia RODO, zabezpieczyć elektroniczne przetwarzanie danych osobowych. Administrator Systemów Informatycznych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Rozdział I. Procedury nadawania, zmiany oraz odbierania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności w poszczególnych systemach przetwarzania danych.

1. Osobą odpowiedzialną za nadawanie uprawnień w systemach informatycznych jest administrator systemu informatycznego.
2. Procedura nadawania, modyfikowania i odbierania uprawnień użytkownikowi w systemach informatycznych obejmuje:
   a) nadanie przez administratora danych upoważnienia do przetwarzania danych w formie tradycyjnej oraz w systemach informatycznych (w tym również dysku sieciowym, programie lub aplikacji, poczcie elektronicznej), a także odebranie oświadczenia o zachowaniu poufności i przestrzeganiu wewnętrznej dokumentacji ochrony danych,
   b) przy nadawaniu przez administratora danych upoważnienia do przetwarzania danych w systemach informatycznych (w tym również dysku sieciowym, programie lub aplikacji, poczcie elektronicznej), użytkownikowi, obowiązuje zasada minimalizacji uprawnień w niezbędnym do wykonywania czynności zakresie,
   c) zwrócenie się Kierownika działu, z wnioskiem do administratora systemów informatycznych o nadanie uprawnień użytkownikowi w systemach informatycznych. Procedura nadania uprawnień użytkownikowi w systemach informatycznych (w tym również dysku sieciowym, programie lub aplikacji, poczcie elektronicznej) została określona w ust.3,
   d) przed nadaniem uprawnień użytkownikowi upoważnionemu do przetwarzania danych administrator systemów informatycznych umożliwia zapoznanie się użytkownikowi z przepisami dotyczącymi ochrony danych w systemach informatycznych oraz procedurami bezpieczeństwa tych systemów,

e) nadanie, zmodyfikowanie lub odbieranie uprawnień użytkownika w systemach informatycznych w niezbędnym zakresie, odbywa się po zweryfikowaniu przez administratora systemów informatycznych treści upoważnienia do przetwarzania danych osobowych pozwalającego na wykonanie czynności zgodnie wydanym upoważnieniem do przetwarzania danych.

3. Procedura nadania uprawnień użytkownikowi w systemach informatycznych, dysku sieciowym, programie lub aplikacji, poczcie elektronicznej, nadawany jest konkretnej osobie jako unikalnemu użytkownikowi i obejmuje w kolejności:

a) utworzenie indywidualnego identyfikatora użytkownika w systemach informatycznych przy zapewnieniu, że identyfikator ten nie był wcześniej przydzielony innemu użytkownikowi,

b) przydzielenie uprawnień dla utworzonego identyfikatora.

4. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
5. Użytkowników obowiązuje zasada pracy na własnym unikalnym identyfikatorze użytkownika.

Rozdział II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (startowe) hasło użytkownika nadawane jest przez administratora systemów informatycznych i przekazywane użytkownikowi z jednoczesnym wymogiem zmiany podczas pierwszego logowania.
2. W przypadku utraty uprawnień przez osobę administrującą systemami informatycznymi należy niezwłocznie zmienić dla takiego identyfikatora hasła, do których miała dostęp.
3. Hasło zastosowane do uwierzytelnienia administratora systemu w systemie informatycznym składa się z co najmniej 8 znaków, w tym musi zawierać małe i duże litery oraz liczbę i znak specjalny.
4. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
5. W przypadku złamania zasady poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora systemów informatycznych.

6. W przypadku logowania przez Centralny System Logowania (CSL) stosowane są metody 2FA (dwuskładnikowe uwierzytelnianie).

Rozdział III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik powinien upewnić się, że wyświetlane na ekranie dane są zabezpieczone w sposób uniemożliwiający dostęp osobom postronnym i nieupoważnionym.
2. Niedozwolone jest wykonywanie jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
3. Przed przerwaniem pracy w systemie informatycznym i tymczasowym odejściem od stanowiska na którym przetwarzane są dane osobowe użytkownik blokuje swój dostęp poprzez manualne uruchomienie blokady systemu komputera.
4. Po zakończeniu pracy użytkownik zamyka system informatyczny, do którego ma dostęp.
5. Komputery w okresie nocnym wyłączane są automatycznie przez Dział IT.

Rozdział IV. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Kopie zapasowe powinny być weryfikowane przez administratora systemów informatycznych, w szczególności pod kątem ich prawidłowości.
2. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.
3. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
4. Kopie zapasowe serwerów (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany dedykowane do tego oprogramowania.
5. Kopie sporządzane są na taśmach magnetycznych oraz w dedykowanych dyskach w serwerach.
6. Dostęp do wydzielonych urządzeń backupowych wraz z nośnikami i oprogramowaniem backupowym mają pracownicy wyznaczeni przez Administratora Systemów Informatycznych po akceptacji Administratora Danych Osobowych.

7. Administrator systemów informatycznych sprawuje nadzór nad poprawnością wykonania kopii zapasowych

8. Kopie zapasowe są składowane na taśmach magnetycznych i przechowywane w sejfie poza pomieszczeniami i poza budynkami, w której umieszczone są maszyny, z których zostały wykonane.

Rozdział V. Sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych,

1. Wszelkie dane osobowe w postaci elektronicznej powinny znajdować się na dyskach serwerów w serwerowniach Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie.
2. Wykaz serwerowni, serwerów wraz z bazami danych osobowych znajduje się w wykazie I.
3. Zabronione jest przechowywanie danych osobowych na dyskach lokalnych stacji roboczych.
4. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności macierze dyskowe / twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone komisyjnie w sposób fizyczny załącznik – protokół zniszczenia uszkodzonych nośników. Stosowana metoda niszczenia, to fizyczne niszczenie wymontowanych nośników.
5. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone zanim zostaną przekazane poza obszar Uczelni.

Rozdział VI. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania.

1. Użytkownicy systemu informatycznego niezwłocznie informują administratora systemu o zagrożeniach wskazywanych przez oprogramowanie antywirusowe.
2. Każdy plik wczytywany do komputera, w tym także wiadomości email, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
3. Należy zabezpieczyć interfejsy urządzeń sieciowych poprzez zmianę domyślnych loginów i haseł/ wyłączenie dostępu zdalnego, gdy nie jest wymagany.

4. W celu zapewnienia bezpieczeństwa nnależy aktualizować oprogramowanie (firmware/ sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, firewalle, macierze).
5. Dokonuje się automatycznej aktualizacji oprogramowania systemów i aplikacji. Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service packi, łatki).
6. Stosuje się system antywirusowy na serwerze, stacjach komputerowych oraz komputerach poza siecią w tym laptopach.
7. W celu ochrony sieci komputerowej stosuje się rozwiązania Firewall
8. Sieć bezprzewodową powinna być zabezpieczona technologią pozwalającą na bezpieczne korzystanie z niej.
9. Zdalny dostęp do sieci komputerowej jest przyznawany wyłącznie przez administratora systemu i odbywa się każdorazowo za jego zgodą. Wykaz osób mających dostęp do sieci stanowi wykaz I.
10. W przypadku podłączeń zdalnych stosuje się technologie VPN zabezpieczoną dodatkowym certyfikatem dostarczanym do komputera służącego do podłączenia się do sieci

Rozdział VII. Procedury wykonywania przeglądów, konserwacji i napraw systemów oraz nośników informacji służących do przetwarzania danych

1. Administrator systemów informatycznych powinien prowadzić okresowe przeglądy systemów informatycznych w celu określania ich poziomu sprawności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz bezpieczeństwo danych przetwarzanych z jego wykorzystaniem.
2. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, przez: administratora systemów informatycznych - firmy zewnętrzne na podstawie zawartych umów. W umowach powinno znajdować się postanowienie o powierzeniu danych osobowych. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora systemów informatycznych.

3. W przypadku konieczności dokonania naprawy elementu infrastruktury systemu informatycznego przez osobę nieupoważnioną (np. zewnętrzny serwis informatyczny) w obszarze przetwarzania danych, wszelkie czynności dokonywane są pod bezpośrednim nadzorem osób upoważnionych lub administratora systemów informatycznych.

Rozdział XI – Postanowienia końcowe

1. Administrator danych osobowych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
2. Wszelkie zasady opisane w niniejszej Instrukcji są przestrzegane przez użytkowników i administratorów systemów ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
3. Nad aktualnością niniejszej Instrukcji odpowiada Administrator Danych Osobowych.
4. Instrukcja obowiązuje od dnia jej zatwierdzenia przez Administratora Danych Osobowych.

Wykaz I.
Wykaz osób mających uprawnienia dostępowe oraz aplikacji wykorzystywanych do połączeń zdalnych.

1. Pracownicy komórki IT KA ciągle.
2. Pracownicy Opteam
3. Pracownicy Bonasoft
4. Pracownicy Biomedic okresowo po ustaleniu i włączeniu dostępu przez IT KA.
5. Pracownicy APR System okresowo po ustaleniu i włączeniu dostępu przez IT KA.

Wykaz II.

Wykaz pomieszczeń do przechowywania kopii bezpieczeństwa

1. Serwerownia główna budynek B pom. B109 streamer.
2. Serwerownia główna budynek A pom. B136 streamer.
3. Serwerownia główna budynek A pom, KASA sejf metalowy.

Załącznik nr 15 do Polityki Bezpieczeństwa Informacji

Zasady „czystego biurka" i „czystego ekranu"
w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie

1. Zasady czystego biurka i czystego ekranu obowiązują wszystkich pracowników zatrudnionych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie i stanowią integralną część Polityki Bezpieczeństwa Informacji.
2. Za pracowników uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, osobę współpracującą z administratorem danych osobowych na podstawie umów cywilnoprawnych, stażystów, praktykantów, wolontariuszy.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. Należy unikać przechowywania dokumentów niepotrzebnych do bieżących zadań. Dokumenty zbędne w danym momencie powinny być przechowywanie w niedostępnym dla osób postronnych miejscu.
4. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.
5. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.
6. Na biurku nie powinny znajdować się napoje w pojemnikach grożących rozlaniem.
7. Po zakończeniu pracy na biurku nie należy pozostawiać dokumentów zawierających dane osobowe.
9. Ekrany monitorów komputerów powinny być ustawione tak by uniemożliwiały dostęp osobom nieupoważnionym.
10. Haseł umożliwiających zalogowanie się, np. do systemu, w żadnym razie nie należy trzymać na biurku, czy w innym ogólnie dostępnym miejscu lub udostępniać osobom nieupoważnionym.
11. Na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty folderów pod warunkiem, że w nazwie nie zawierają informacji zawierających dane osobowe.
13. Pracownik jest zobowiązany do ustawienia wygaszacza ekranu na użytkowanym przez siebie komputerze. Wygaszacz powinien włączać się automatycznie po okresie bezczynności użytkownika, trwającym nie dłużej niż 5 minut. W przypadku wznowienia aktywności, powrót do pracy z komputerem powinien być możliwy jedynie po podaniu odpowiedniego hasła.
14. W przypadku czasowego opuszczenia stanowiska pracy, pracownik jest zobowiązany do każdorazowego blokowania komputera poprzez włączenie wygaszacza ekranu.
15. Po zakończeniu pracy pracownik powinien wylogować się ze wszystkich systemów, (obowiązek wylogowania dotyczy również poczty elektronicznej), zamknąć w szafach dokumenty zawierające dane osobowe lub inne tajemnice ustawowo chronione.
16. Niedopuszczalne jest pozostawianie niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim osoba uprawniona. Zasada nie dotyczy pomieszczeń ogólnie dostępnych. Po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zgodnie z obowiązującymi ustaleniami, zabezpieczyć klucze do pomieszczenia.
17. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji. Dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych

powinny być niszczone w sposób uniemożliwiający ich odczytanie w niszczarce. Niszczenie takich dokumentów powinno odbywać się w miarę możliwości na bieżąco.

Załącznik nr 16 do Polityki Bezpieczeństwa Informacji

Kraków dn. .....

.....
Imię i nazwisko

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

w oparciu o wymogi Rozporządzenia ogólnego o ochronie danych z dnia 27 kwietnia 2016 r. (RODO)

Wyrażam zgodę na przetwarzanie moich danych osobowych, w celu zrealizowania zawartej umowy przez Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie (z siedzibą w Krakowie ul. Gustawa Herlinga-Grudzińskiego 1 w Krakowie), który będzie Administratorem Danych Osobowych.

.....

(czytelny podpis)

Wyrażam zgodę na:

2.	Wykorzystanie udostępnionego przeze mnie:		
	Adresu e-mail	TAK	NIE
	Nr telefonu:	TAK	NIE
3.	na nieodpłatne rozpowszechnianie mojego wizerunku przez Krakowską Akademię im. Andrzeja Frycza Modrzewskiego z siedzibą w Krakowie, przy ul. Gustawa Herlinga-Grudzińskiego 1, utrwalonego w postaci zdjęć przedstawiających moją osobę wykonanych przez pracowników Uczelni, zamieszczonych w materiałach informacyjnych i promocyjnych dotyczących Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, w publikacjach prasowych oraz na stronach internetowych i portalach społecznościowych, bez ograniczeń terytorialnych i czasowych	TAK	NIE

.....

(czytelny podpis)

Przyjmuję do wiadomości, że :

1. Podanie danych osobowych jest dobrowolne, lecz odmowa ich podania jest równoznaczna z brakiem możliwości zawarcia umowy.
2. Mam prawo dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; wycofanie zgody na przetwarzanie danych osobowych można przesłać e-mailem na adres: iodo@afm.edu.pl
3. Mam prawo do wniesienia skargi do organu nadzorczego ochrony danych osobowych.
4. Dane osobowe mogą zostać udostępnione innym podmiotom wyłącznie posiadającym odpowiednie upoważnienie na podstawie przepisów prawa krajowego lub unijnego.
5. Udostępnione dane osobowe nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu oraz nie będą przekazane do państwa trzeciego lub organizacji międzynarodowej.
6. Moje dane osobowe będą przetwarzane przez czas realizacji umowy oraz przez czas niezbędny do ewentualnych postępowań wyjaśniających.
7. Z Inspektorem Ochrony Danych Osobowych nadzorującym prawidłowość przetwarzania w. w. danych osobowych można skontaktować się pod adresem e-mail: iodo@afm.edu.pl

Zapoznałem się z klauzulą informacyjną .....

(czytelny podpis)

Jednocześnie zobowiązuję się w trakcie trwania umowy o pracę/umowy zlecenia*/o dzieło*, jak i po jej ustaniu, do zachowania*
w tajemnicy wszelkich danych osobowych do których mam i będę miał/ miała dostęp w związku z wykonywaniem obowiązków służbowych. (*niepotrzebne skreślić).

Table: OSOBA

Fields

Name	Type	Domain	Not Null
OSOBA_ID	INTEGER	RDB$1403	NOT NULL
MIASTO_ID	INTEGER	RDB$1404	
OBYWATELSTWO_ID	INTEGER	RDB$1405	
NAROD_ID	INTEGER	RDB$1406	
KRAJPOCH_ID	INTEGER	RDB$1407	
OSOBA_TYP	CHAR(1)	RDB$1408	
OSOBA_NAZWISKO	VARCHAR(50)	RDB$1409	
OSOBA_IMIE	VARCHAR(30)	RDB$1410	
OSOBA_IMIE2	VARCHAR(50)	RDB$1411	
OSOBA_PLEC	CHAR(1)	RDB$1412	
OSOBA_DATAUR	DATE	RDB$1413	
OSOBA_MIEJSCEUR	VARCHAR(50)	RDB$1414	
OSOBA_ADRULICA	VARCHAR(40)	RDB$1415	

OSOBA_ADRKODP	VARCHAR(7)	RDB$1416	

Date / Time: User: **APRSYSTEM**
Database: Table: **OSOBA**

OSOBA_GMINA	VARCHAR(30)	RDB$1417	
OSOBA_NRALBP	VARCHAR(10)	RDB$1418	
OSOBA_NRALB	INTEGER	RDB$1419	
OSOBA_NRALBS	VARCHAR(15)	RDB$1420	
OSOBA_KORULICA	VARCHAR(40)	RDB$1421	
OSOBA_KORKODP	VARCHAR(7)	RDB$1422	
OSOBA_KORGMINA	VARCHAR(30)	RDB$1423	
OSOBA_TELKOM	VARCHAR(50)	RDB$1424	
OSOBA_TELEFON1	VARCHAR(20)	RDB$1425	
OSOBA_TELEFON2	VARCHAR(20)	RDB$1426	
OSOBA_ZDJECIE	BLOB SUB_TYPE 0 SEGMENT SIZE 80	BLOB_SUB_TYPE_A	
OSOBA_LOGIN	VARCHAR(50)	RDB$1427	

OSOBA_HASLO	VARCHAR(40)	RDB$1428	
OSOBA_HASLON	VARCHAR(200)	RDB$1429	
OSOBA_INT	CHAR(1)	RDB$1430	

Date / Time: User: **APRSYSTEM**
Database: Table: **OSOBA**

OSOBA_POWIAD	INTEGER	RDB$1431	
OSOBA_QUOTA	INTEGER	RDB$1432	
OSOBA_HOMEPATH	VARCHAR(30)	RDB$1433	
OSOBA_VP	CHAR(1)	RDB$1434	
OSOBA_LOGINVP	VARCHAR(20)	RDB$1435	
OSOBA_HASLOVP	VARCHAR(20)	RDB$1436	
OSOBA_ZRODLODANYCH	VARCHAR(100)	RDB$1437	
OSOBA_SPRZECIWUDDO	CHAR(1)	RDB$1438	
OSOBA_KODKRESK	VARCHAR(150)	RDB$1439	

OSOBA_PESEL	VARCHAR(15)	RDB$1440	
OSOBA_NIP	VARCHAR(20)	RDB$1441	
OSOBA_SERIADOW	VARCHAR(5)	RDB$1442	
OSOBA_NRDOW	VARCHAR(20)	RDB$1443	
OSOBA_NRDOWWYDANY	VARCHAR(200)	RDB$1444	
OSOBA_PASZPORT	VARCHAR(30)	RDB$1445	

OSOBA_EMAILPRYW	VARCHAR(50)	RDB$1446	
OSOBA_EMAILUCZ	VARCHAR(250)	RDB$1447	
OSOBA_WWW	VARCHAR(100)	RDB$1448	
OSOBA_DANE1	VARCHAR(100)	RDB$1449	
OSOBA_DANE2	VARCHAR(100)	RDB$1450	
OSOBA_DANE3	VARCHAR(100)	RDB$1451	

OSOBA_DANE4	VARCHAR(100)	RDB$1452	
OSOBA_POPRDANEOS	CHAR(1)	RDB$1453	
OSOBA_POPRZDJECIE	CHAR(1)	RDB$1454	
OSOBA_POPRKONTO	CHAR(1)	RDB$1455	
OSOBA_DATAWAZN	DATE	RDB$1456	
KMODINS	VARCHAR(20)	RDB$1457	
DMODINS	DATE	RDB$1458	
KMOD	VARCHAR(20)	RDB$1459	
DMOD	TIMESTAMP	RDB$1460	

OSOBA_ZMIANAHASLA	CHAR(1)	RDB$1461	
OSOBA_WDLICZBALOGOWAN	INTEGER	RDB$1462	
MIASTO_IDKOR	INTEGER	RDB$1463	

OSOBA_ANKIETER	CHAR(1)	RDB$1464	
OSOBA_DODANAPRZEZBK	CHAR(1)	RDB$1465	
OptimisticLockField	INTEGER	RDB$1467	
OSOBA_POPRDANEREK	CHAR(1)	RDB$4916	
KRAJ_WYDDOKID	INTEGER	RDB$4162	
OSOBA_TEMP	BLOB SUB_TYPE 0 SEGMENT SIZE 80	BLOB_SUB_TYPE_A	
OSOBA_STATUSKREM	INTEGER	RDB$4931	
OSOBA_UWAGI	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
OSOBA_DATAWAZNDOW	DATE	RDB$5270	
OSOBA_DATAWAZNPASZPORT	DATE	RDB$5271	
DSYNCHSIMPLE	TIMESTAMP	RDB$6395	
OSOBA_PREFKIER	INTEGER	RDB$6445	

JEZYK_ID	INTEGER	RDB$6443	
OSOBA_RODZAJMIEJSC	INTEGER	RDB$6510	
OSOBA_LOG	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
OSOBA_UIDPOLON	VARCHAR(128)	RDB$6756	
OSOBA_MIEJSCEURTL	VARCHAR(1000)	RDB$7196	
Computed Source: ((SELECT COALESCE(TEKSTTLVC, OSOBA_MIEJSCEUR) FROM OG_DAJTLUMACZENIE(OSOBA_ID, 12,18)))			
OSOBA_SPOSOBPRZYPHASLA	INTEGER	RDB$7241	
OSOBA_TOKENHASH	VARCHAR(64)	RDB$7248	
OSOBA_TOKENWAZNOSC	TIMESTAMP	RDB$7249	
STATREKR_ID	INTEGER	RDB$7288	
OSOBA_POTW	INTEGER	RDB$7290	
Computed Source: ((select STATREKR_KOD from STATREKR where STATREKR.STATREKR_ID = OSOBA.STATREKR_ID))			
OSOBA_ASAPTOKENHASH	VARCHAR(64)	RDB$7472	
OSOBA_ASAPTOKENWAZN	TIMESTAMP	RDB$7473	
OSOBA_PODSTSTPOSIADAKARTEPOLAKA	CHAR(1)	RDB$7773	

OSOBA_PODSTSTREPATRIANT	CHAR(1)	RDB$7774	

OSOBA_PODSTSTPOWODKWALCUDZOZ	CHAR(1)	RDB$7775	
OSOBA_DATAWAZNHASLA	DATE	RDB$8181	

Table: STUD

Fields

Name	Type	Domain	Not Null
STUD_ID	INTEGER	RDB$2718	NOT NULL
STAT_ID	INTEGER	RDB$2719	NOT NULL
LICEUM_ID	INTEGER	RDB$2720	
SPEC_ID	INTEGER	RDB$2721	NOT NULL
STUDIA_ID	INTEGER	RDB$2722	NOT NULL
UCZUK_ID	INTEGER	RDB$2723	
KIERUK_ID	INTEGER	RDB$2724	
KOMENDA_ID	INTEGER	RDB$2725	

TKONTMAS_ID	INTEGER	RDB$2726	
SEMUCZ_ID	INTEGER	RDB$2727	NOT NULL
SPECUK_ID	INTEGER	RDB$2728	
TYTULDLUG_ID	INTEGER	RDB$2729	NOT NULL
SWIADECTWOWYD_ID	INTEGER	RDB$2730	
AKADEMIK_ID	INTEGER	RDB$2731	

KOLOR_ID	INTEGER	RDB$2732	
OSOBA_ID	INTEGER	RDB$2733	
TOKNAUKI_ID	INTEGER	RDB$2734	
STUD_NRUMOWY	VARCHAR(30)	RDB$2735	
STUD_DATAUMOWY	DATE	RDB$2736	
STUD_NRALBUMUP	VARCHAR(10)	RDB$2737	
STUD_NRALBUMU	INTEGER	RDB$2738	

STUD_NRALBUMUS	VARCHAR(15)	RDB$2739	
STUD_NRLEGP	VARCHAR(10)	RDB$2740	
STUD_NRLEG	INTEGER	RDB$2741	
STUD_NRLEGS	VARCHAR(15)	RDB$2742	
STUD_IMMATKI	VARCHAR(20)	RDB$2743	
STUD_IMOJCA	VARCHAR(20)	RDB$2744	
STUD_NAZWPAN	VARCHAR(30)	RDB$2745	
STUD_NAZWPANMATKI	VARCHAR(40)	RDB$2746	

STUD_STCYWILNY	VARCHAR(5)	RDB$2747	
STUD_MPRACY	VARCHAR(70)	RDB$2748	
STUD_OKRESPRACY	VARCHAR(30)	RDB$2749	
STUD_SWIADECTWO	VARCHAR(50)	RDB$2750	

STUD_DATAROZP	DATE	RDB$2751	
STUD_GENRECZN	CHAR(1)	RDB$2752	
STUD_OPISCZ	VARCHAR(100)	RDB$2753	
STUD_DATAZAK	DATE	RDB$2754	
STUD_ROKST	INTEGER	RDB$2755	
STUD_SEMESTR	INTEGER	RDB$2756	
STUD_INDYW	CHAR(1)	RDB$2757	
STUD_ROKUKLO	INTEGER	RDB$2758	
STUD_STOSSLWOJSK	INTEGER	RDB$2759	
STUD_NRKSWOJ	VARCHAR(15)	RDB$2760	
STUD_KATWOJSKOWA	VARCHAR(3)	RDB$2761	

STUD_MAAKADEMIK	CHAR(1)	RDB$2762	

STUD_STYPENDIUM	DOUBLE PRECISION	RDB$2763	
STUD_SREDNIA	DOUBLE PRECISION	RDB$2764	
STUD_KONTOSTUD	VARCHAR(50)	RDB$2765	
STUD_BANKSTUD	VARCHAR(50)	RDB$2766	
STUD_NAZWAPL1	VARCHAR(50)	RDB$2767	
STUD_NAZWAPL2	VARCHAR(50)	RDB$2768	
STUD_ULICAPL	VARCHAR(30)	RDB$2769	
STUD_KODPPL	VARCHAR(6)	RDB$2770	
STUD_MIASTOPL	VARCHAR(30)	RDB$2771	
STUD_NIPPL	VARCHAR(15)	RDB$2772	
STUD_UWAGI	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_STYPSOC	DOUBLE PRECISION	RDB$2773	
STUD_DATAUKSTLIC	DATE	RDB$2774	
STUD_NRDYPLSTUDLIC	VARCHAR(100)	RDB$2775	

Date / Time: **31 styczeń 2019** User: **APRSYSTEM**
Database: Table: **STUD**

STUD_KONTOUCZSTUD	VARCHAR(50)	RDB$2777	
STUD_DATAPRZJECIA	DATE	RDB$2778	
STUD_PRZESWZAPLACIE	INTEGER	RDB$2779	
STUD_UWAGICZ	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_DATAODEBRDOK	DATE	RDB$2780	
STUD_DATASWDOJ	DATE	RDB$2781	
STUD_PRAKTYKA	CHAR(1)	RDB$2782	
STUD_CZASTRWPRAKT	INTEGER	RDB$2783	
STUD_DATADYPLIC	DATE	RDB$2784	
STUD_SUPDODINF	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_SUPINDYWOS	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_SUPPOSKWAL	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_SUPNAZWAUCZ	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_WARPRZYJ	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	

STUD_STANDNAUCZ	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	

Date / Time: **31 styczeń 2019** User: **APRSYSTEM**
Database: Table: **STUD**

STUD_DALSZEZRINF	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_ILPUNKTOW	DOUBLE PRECISION	RDB$2785	
STUD_NRTECZKI	INTEGER	RDB$2786	
STUD_INNEUCZELNIE	VARCHAR(100)	RDB$2787	
STUD_TYPWYPSTYP	CHAR(1)	RDB$2788	
STUD_ROZLCZESNE	CHAR(1)	RDB$2789	
STUD_DOSWZAW	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_OCENAPRAKTYK	VARCHAR(5)	RDB$2790	
STUD_DATADECKOMISJI	DATE	RDB$2791	
KMOD	VARCHAR(20)	RDB$2792	
DMOD	TIMESTAMP	RDB$2793	

KMODINS	VARCHAR(20)	RDB$2794	
DMODINS	TIMESTAMP	RDB$2795	
LINK	VARCHAR(8)	RDB$2796	
KODBAZY	VARCHAR(3)	RDB$2797	

DATAEGZAMINULICINZ	TIMESTAMP	RDB$2798	
OCENAEGZAMINULICINZ	FLOAT	RDB$2799	
OCENAPRACYLICINZ	FLOAT	RDB$2800	
OCENAPRACYLICINZ1	FLOAT	RDB$2801	
OCENAPRACYLICINZ2	FLOAT	RDB$2802	
DATAPRACYLICINZ	TIMESTAMP	RDB$2803	
NUMERDYPLOMULICINZ	VARCHAR(50)	RDB$2804	
APRLOCKDATA	CHAR(1)	RDB$2805	

STUD_ARCH	CHAR(1)	RDB$2806	
STUD_UWAGIPRAKTYKA	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_SEMESTRPRZYJ	INTEGER	RDB$2807	
ZRUTRZYMANIA_ID	INTEGER	RDB$2808	
STUD_STAWKAECTS	DOUBLE PRECISION	RDB$2809	
OptimisticLockField	INTEGER	RDB$2810	
STUD_KOLEJNOSCKIER	INTEGER	RDB$4919	

STUD_KOMPLETDOK	CHAR(1)	RDB$3917	
STUD_ADRRODZICOW	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_ZAMELD	CHAR(1)	RDB$4118	
STUD_NRKARTYMIESZK	VARCHAR(35)	RDB$4159	
STUD_PIERWSZYKIER	CHAR(1)	RDB$4163	

STUD_ZWOLNIONYZOPLAT	CHAR(1)	RDB$4164	
STUD_NRKMIESZKDATAGEN	DATE	RDB$4327	
STUD_SUPLCZASTRWANIA	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_ILPUNKTOWKREM	DOUBLE PRECISION	RDB$4900	
STUD_MIEJSCEWYSTLO	VARCHAR(100)	RDB$5029	
STUD_MIEJSCEWYSTUCZ	VARCHAR(100)	RDB$5030	
STUD_REKINT	CHAR(1)	RDB$5031	
RODZMATURY_ID	INTEGER	RDB$5191	
STUD_OPISREKR	VARCHAR(200)	RDB$5072	
STUD_WSPOLNEWPISOWE	INTEGER	RDB$5080	

STUD_ODPISDYPL	CHAR(1)	RDB$5259	
STUD_NOWAREKUZPOPROCENY	CHAR(1)	RDB$5175	

STUD_WYSLANOPOWREK	CHAR(1)	RDB$6261	
STUD_DATAPRZYJNAKIER	DATE	RDB$6302	
DSYNCHSIMPLE	TIMESTAMP	RDB$6394	
STUD_ROBOCZE	INTEGER	RDB$6505	
STUD_ILPUNKTOWWER	DOUBLE PRECISION	RDB$6545	
STUD_NOTATKA	VARCHAR(250)	RDB$6533	
STUD_KIERUNEKUZUPID	VARCHAR(8)	RDB$6552	
STUD_DUPLIKATDYPL	CHAR(1)	RDB$6578	
STUD_SPROSTOWANIA	BLOB SUB_TYPE 1 SEGMENT SIZE 80	BLOB_SUB_TYPE_B	
STUD_SUPNAZWAUCZTL	BLOB SUB_TYPE 1	RDB$7207	
Computed Source:	((SELECT COALESCE(TEKSTTLBL, STUD_SUPNAZWAUCZ) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,8)))		
STUD_WARPRZYJTL	BLOB SUB_TYPE 1	RDB$7208	
Computed Source:	((SELECT COALESCE(TEKSTTLBL, STUD_WARPRZYJ) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,9)))		

Database: Table: **STUD**

STUD_STANDNAUCZTL	BLOB SUB_TYPE 1	RDB$7209	
Computed Source: ((SELECT COALESCE(TEKSTTLBL, STUD_STANDNAUCZ) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,10)))			
STUD_SUPPOSKWALTL	BLOB SUB_TYPE 1	RDB$7210	
Computed Source: ((SELECT COALESCE(TEKSTTLBL, STUD_SUPPOSKWAL) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,12)))			
STUD_SUPINDYWOSTL	BLOB SUB_TYPE 1	RDB$7211	
Computed Source: ((SELECT COALESCE(TEKSTTLBL, STUD_SUPINDYWOS) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,11)))			
STUD_SUPDODINFTL	BLOB SUB_TYPE 1	RDB$7212	
Computed Source: ((SELECT COALESCE(TEKSTTLBL, STUD_SUPDODINF) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,13)))			
STUD_DALSZEZRINFTL	BLOB SUB_TYPE 1	RDB$7213	
Computed Source: ((SELECT COALESCE(TEKSTTLBL, STUD_DALSZEZRINF) FROM OG_DAJTLUMACZENIE(STUD_ID, 8,14)))			
STATREKR_ID	INTEGER	RDB$7289	
STUD_STATUSREK	BIGINT	RDB$7291	
Computed Source: ((select (STATREKR_KOD-4) from STATREKR where STATREKR.STATREKR_ID = STUD.STATREKR_ID))			
ZMIANADANYCH_ID	INTEGER	RDB$7364	
STUD_WYSLANOPOWREKWPLATAWPIS	CHAR(1)	RDB$7365	

STUD_ZWOLNIONYZOPLATYWPIS	CHAR(1)	RDB$7417	

Date / Time: User: **APRSYSTEM**
Database: Table: **STUD**

STUD_KODQR	BLOB SUB_TYPE 0 SEGMENT SIZE 80	RDB$7464	
PROW_ID	INTEGER	RDB$8476	

Załącznik nr 18 do Polityki Bezpieczeństwa Informacji

INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH
(proces rekrutacji)

Zgodnie z art. 13 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 (…) („Rozporządzenie Ogólne") Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie informuje, iż:

I. Administratorem Pani/Pana danych osobowych jest Uniwersytet Andrzej Frycza Modrzewskiego w Krakowie, ul. Gustawa Herlinga Grudzińskiego 1, 30-705 Kraków.

II. Uczelnia powołała Inspektora Ochrony Danych Osobowych, z którym może się Pani/Pan skontaktować w przypadku jakichkolwiek pytań lub uwag dotyczących przetwarzania Pani/Pana danych osobowych, przy ul. Gustawa Herlinga-Grudzińskiego 1 w Krakowie lub za pośrednictwem adresu e-mail: iodo@afm.edu.pl.

III. Pani/Pana dane osobowe będą przetwarzane w celu przeprowadzenia procedury rekrutacyjnej, a w razie przyjęcia do pracy w związku z wykonywaniem umowy o pracę.

IV. Pani/Pana dane osobowe w zakresie wskazanym w przepisach prawa pracy będą przetwarzane w celu przeprowadzenia obecnego postępowania rekrutacyjnego (art. 6 ust. 1 lit. b RODO), natomiast inne dane, w tym dane do kontaktu, na podstawie zgody (art. 6 ust. 1 lit. a RODO), która może zostać odwołana w dowolnym czasie.
Przepisy prawa pracy: art. 22 [1] Kodeksu pracy oraz §1 rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.

V. Podanie przez Pana/Panią danych osobowych jest dobrowolne, lecz konieczne do uczestnictwa w procedurze rekrutacyjnej. Konsekwencją niepodania danych osobowych będzie brak możliwości udziału w rekrutacji.

VI. Pani/Pana dane osobowe będą przechowywane przez okres: do czasu zakończenia procedury rekrutacji, a w razie zawarcia umowy o pracę po jej wygaśnięciu w celach archiwalnych.

VII. Pani/Pana dane osobowe nie będą przekazywane do państw trzecich oraz do organizacji międzynarodowych.

VIII. Posiada Pani/Pan prawo do: dostępu do treści swoich danych oraz ich sprostowania, a także prawo do usunięcia, ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu wobec przetwarzania – w przypadkach i na warunkach określonych w Rozporządzeniu Ogólnym (RODO).

IX. Posiada Pani/Pan również prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Wycofanie zgody na przetwarzanie danych osobowych można przesłać e-mailem na adres: iodo@afm.edu.pl lub pocztą tradycyjną na adres: ul. Gustawa Herlinga Grudzińskiego 1, 30-705 Kraków.

X. Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza przepisy Rozporządzenia Ogólnego.

Potwierdzam, że zapoznałem(am) się i przyjmuję do wiadomości powyższe informacje.

……
Miejscowość, data, czytelny podpis

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb niezbędnych do realizacji procesu rekrutacji, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych 10 maja 2018 r. o ochronie danych osobowych Dz. U. z dnia 24 maja 2018 r., poz. 1000 oraz zgodnie klauzulą informacyjną dołączoną do mojej zgody.

…….

Miejscowość, data, czytelny podpis

Załącznik nr 19 do Polityki Bezpieczeństwa Informacji

Kraków, dnia.....

ZGODA NA ROZPOWSZECHNIANIE WIZERUNKU

Ja, niżej podpisany/a ....., zamieszkały/a w ..... przy ul. ..... wyrażam zgodę na nieodpłatne rozpowszechnianie mojego wizerunku przez Uniwersyte Andrzeja Frycza Modrzewskiego w Krakowie z siedzibą w Krakowie, przy ul. Gustawa Herlinga-Grudzińskiego 1, utrwalonego w postaci zdjęć/ materiałów filmowych przedstawiających moją osobę wykonanych przez pracowników Uczelni w ramach …….. (*np. inicjatywa/ wydarzenie w trakcie, którego miałoby dojść do wykonywania ww. zdjęć/ materiałów filmowych*), zamieszczonych w materiałach informacyjnych i promocyjnych dotyczących Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie, w publikacjach prasowych, bez ograniczeń terytorialnych i czasowych.

Zgoda obejmuje: wykorzystanie, utrwalenie, edycję, obróbkę, powielanie oraz tworzenie kopii zapasowych zarejestrowanych materiałów filmowych oraz wykonanych zdjęć przedstawiających jego osobę, jak również publiczne rozpowszechnienie materiałów filmowych oraz udostępnienie wykonanych fotografii w publikacjach prasowych, np. w dziennikach, czasopismach okresowych, czasopismach okazjonalnych gdzie publikowana jest informacja o Uczelni, a także udostępnienie fotografii i materiałów filmowych – na stronach internetowych Uczelni, na stronach gdzie zamieszczana jest informacja o Uczelni, w szczególności na: portalach edukacyjnych, portalach informacyjnych, portalach społecznościowych (np.: Facebook, Instagram, X, LinkedIn), oraz na innych stronach internetowych, na których podawane są do publicznej wiadomości przez Uczelnie materiały fotograficzne i filmowe, np.: w portalu „YouTube”, a także zamieszczanie w materiałach promocyjnych i informacyjnych Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie w formie papierowej i na nośnikach danych np. cd/dvd/usb oraz umieszczanie w formie elektronicznej „online” na stronie internetowej Uczelni. Osoba przyjmuje do wiadomości, że zarejestrowane materiały filmowe lub wykonane fotografie przedstawiające jego osobę mogą zostać przekazane partnerom lub współorganizatorom wydarzenia w celu udostępnienia ich np. na stronie internetowej, na portalach społecznościowych partnerów lub współorganizatorów.

.....

(czytelny podpis)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH
w oparciu o wymogi Rozporządzenia ogólnego o ochronie danych z dnia 27 kwietnia 2016 r. (RODO)

Wyrażam zgodę na przetwarzanie moich danych osobowych, w celu potwierdzenia prawa do rozpowszechniania mojego wizerunku przez Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie z siedzibą przy ul. Gustawa Herlinga-Grudzińskiego 1 w Krakowie.

…….
(czytelny podpis)

Informacja dotycząca przetwarzania danych osobowych

Zgodnie z art. 13 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 (…) („Rozporządzenie Ogólne") Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie informuje, iż:

I. Administratorem Pani/Pana danych osobowych jest Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie, ul. Gustawa Herlinga Grudzińskiego 1, 30-705 Kraków.
II. Uczelnia powołała Inspektora Ochrony Danych Osobowych, z którym może się Pani/Pan skontaktować w przypadku jakichkolwiek pytań lub uwag dotyczących przetwarzania Pani/Pana danych osobowych, przy ul. Gustawa Herlinga-Grudzińskiego 1 w Krakowie lub za pośrednictwem adresu e-mail:iodo@afm.edu.pl.
III. Pani/Pana dane osobowe, w tym Pani/Pana wizerunek, przetwarzane będą do celów związanych z promocją Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie, na podstawie art. 6 ust. 1 lit. a Rozporządzenia Ogólnego, wyłącznie w przypadku gdy wyrazi Pani/Pan zgodę na publikację wizerunku, wynikającą z art. 81 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.
IV. Wyrażenie zgody na przetwarzanie danych osobowych, w tym Pani/Pana wizerunku jest dobrowolne, a jej niewyrażenie jest równoznaczne z brakiem możliwości utrwalenia Pani/Pana wizerunku.
V. Pani/Pana dane osobowe mogą być przekazane lub udostępnione wyłącznie podmiotom uprawnionym do tego na podstawie przepisów prawa.
VI. Pani/Pana dane osobowe, w tym Pani/Pana imię, nazwisko, wizerunek będą przechowywane przez okres korzystania ze zdjęć i materiałów filmowych oraz przez czas niezbędny do ewentualnych postępowań wyjaśniających (dochodzenia roszczeń).
VII. Posiada Pani/Pan prawo do: dostępu do treści swoich danych oraz ich sprostowania, a także prawo do usunięcia, ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu wobec przetwarzania – w przypadkach i na warunkach określonych w Rozporządzeniu Ogólnym.
VIII. Posiada Pani/Pan również prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Wycofanie zgody na przetwarzanie wizerunku można przesłać e-mailem na adres: iodo@afm.edu.pl lub pocztą tradycyjną na adres: ul. Gustawa Herlinga Grudzińskiego 1, 30-705 Kraków.
IX. Pani/Pana dane osobowe, w tym Pani/Pana wizerunek nie będą przekazywane do organizacji międzynarodowych, jak również nie będą podlegały profilowaniu.
X. Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza przepisy Rozporządzenia Ogólnego.

…….
(czytelny podpis)

Załącznik nr 20 do Polityki Bezpieczeństwa Informacji

Raport z naruszenia ochrony danych osobowych

Sporządzający raport:
Imię i nazwisko .....
stanowisko (funkcja) .....
Dział, pokój, nr telefonu .....

Zgłaszający naruszenie:
Imię i nazwisko .....
stanowisko (funkcja) .....
Dział, pokój, nr telefonu .....

Formy naruszenia ochrony danych .....
miejsce, dokładny czas i data stwierdzenia naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):
.....
.....

1) osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):
.....
.....
2) osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:
.....
.....
3) informacje o danych, które zostały lub mogły zostać ujawnione:
.....
.....
4) zabezpieczone materiały lub inne dowody związane z wydarzeniem:
.....
.....
5) krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):
.....
.....
6) postępowanie wyjaśniające i naprawcze (zalecenia):
.....
.....

…… …….
(data i podpis pracownika) (data i podpis Inspektora Ochrony Danych Osobowych)

Załącznik nr 21 do Polityki Bezpieczeństwa Informacji

Wykaz typowych zagrożeń (ryzyk) dla ochrony danych osobowych

Zniszczenia fizyczne:

1) Pożar;
2) Zalanie
3) Zanieczyszczenie
4) Poważny wypadek;
5) Zniszczenie urządzeń lub nośników;
6) Pył, korozja, wychłodzenie

Zjawiska naturalne:

1) Zjawiska klimatyczne;
2) Powódź;
3) Zjawiska pogodowe;
4) Zjawiska sejsmiczne

Utrata podstawowych usług:

1) Awaria systemu klimatyzacji;
2) Brak dostaw wody;
3) Utrata dostaw prądu;
4) Awaria urządzenia telekomunikacyjnego

Działanie osób trzecich na szkodę organizacji:

1) Przechwycenie sygnałów na skutek zjawiska interferencji ;
2) Szpiegostwo zdalne;
3) Podsłuch;
4) Kradzież nośników lub dokumentów;
5) Kradzież urządzenia;
6) Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników;
7) Ujawnienie informacji;
8) Dane z niewiarygodnych źródeł;
9) Manipulowanie urządzeniem;
10) Podrobienie oprogramowania

Awarie techniczne:

1) Awaria urządzenia;
2) Niewłaściwe funkcjonowanie urządzeń;
3) Przeciążenie systemu informatycznego;
4) Niewłaściwe funkcjonowanie oprogramowania;
5) Naruszenie zdolności utrzymania systemu informatycznego

Nieautoryzowane działania:

1) Nieautoryzowane użycie urządzeń;
2) Nieuprawnione kopiowanie oprogramowania;
3) Użycie podrobionego lub skopiowanego oprogramowania;
4) Zniekształcenie danych;
5) Nielegalne przetwarzanie danych

Naruszenie bezpieczeństwa funkcji:

1) Błąd użytkowania;
2) Naruszenie praw;
3) Przejęcie uprawnień;
4) Odmowa działania;
5) Naruszenie dostępności personelu