Zarządzenie nr 11
Rektora Uniwersytetu w Białymstoku
z dnia 16 kwietnia 2019 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym w Uniwersytecie w Białymstoku

Na podstawie art. 23 ust. 2 pkt 2 ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2018 r., poz. 1668 z późn. zm.), art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016 r.) oraz ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. z 2018 r., poz. 1000 z późn. zm.) zarządza się, co następuje:

§ 1

1. Wprowadza się Politykę bezpieczeństwa danych osobowych w Uniwersytecie w Białymstoku, stanowiącą Załącznik nr 1 do niniejszego Zarządzenia.
2. Zobowiązuje się pracowników, studentów i doktorantów Uniwersytetu w Białymstoku do zapoznania się z Polityką, o której mowa w ust. 1, oraz stosowania jej zasad.

§ 2

1. Wprowadza się Instrukcję zarządzania systemem informatycznym w Uniwersytecie w Białymstoku, stanowiącą Załącznik nr 2 do niniejszego Zarządzenia.
2. Instrukcja, o której mowa w ust. 1, stanowi dokument do użytku wewnętrznego i nie podlega upublicznieniu. Pracownicy Uniwersytetu w Białymstoku są zobowiązani do utrzymania w poufności opisu zabezpieczeń w niej ujętych.
3. Zobowiązuje się kierowników jednostek organizacyjnych Uniwersytetu w Białymstoku do zapoznania podległych im pracowników z Instrukcją, o której mowa w ust. 1, i zapewnienia stosowania jej wytycznych.

§ 3

1. Traci moc:
   1) Zarządzenie nr 3 Rektora Uniwersytetu w Białymstoku z dnia 14 marca 2012 r. *w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych Uniwersytetu w Białymstoku.*
   2) Zarządzenie nr 6 Rektora Uniwersytetu w Białymstoku z dnia 16.02.2004 r. *w* sprawie *ochrony danych osobowych w systemach informatycznych Uniwersytetu w Białymstoku.*
2. Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
UNIWERSYTETU w BIAŁYMSTOKU
prof. dr hab. Robert W. Ciborowski

Załącznik nr 1
do Zarządzenia nr 11
Rektora Uniwersytetu w Białymstoku
z dnia 16 kwietnia 2019 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W UNIWERSYTECIE W BIAŁYMSTOKU

Rozdział I
PRZEDMIOT POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Polityka bezpieczeństwa danych osobowych w Uniwersytecie w Białymstoku stanowi zbiór procedur dotyczących realizacji obowiązków Administratora danych osobowych względem podmiotów danych oraz organu nadzorczego sformułowanych w *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*. Polityka jest wyrazem świadomości Administratora danych osobowych w zakresie zagrożeń wynikających z przetwarzania danych osobowych pracowników, studentów i doktorantów na dużą skalę oraz rozwoju incydentów bezpieczeństwa wynikających z przetwarzania danych w systemach informatycznych.

Polityka określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane proporcjonalnie do zidentyfikowanych możliwości wystąpienia ryzyka, takich jak możliwość udostępnienia danych osobom nieupoważnionym, ich nieuprawniona zmiana, utrata, uszkodzenie, zniszczenie lub przywłaszczenie, a także przetwarzanie niezgodnie z przepisami ww. rozporządzenia i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Polityka skierowana jest do pracowników Uniwersytetu zatrudnionych przy przetwarzaniu danych osobowych, do osób współpracujących z Uniwersytetem przy przetwarzaniu danych osobowych oraz do studentów i doktorantów przetwarzających dane osobowe w związku z pełnieniem funkcji związanych z działalnością Uniwersytetu, w tym funkcji samorządowych.

1. Ilekroć w niniejszej Polityce jest mowa o:
   1) Administratorze systemów informatycznych, zwanym dalej ASI – należy przez to rozumieć osoby odpowiedzialne w Uniwersytecie za zarządzanie aplikacjami komputerowymi, sprzętem i sieciami.
   2) Administratorze danych osobowych, zwanym dalej Administratorem danych lub ADO – należy przez to rozumieć Uniwersytet w Białymstoku.
   3) Danych osobowych – rozumie się przez to informacje zgodne z definicją zawartą w art. 4 pkt 1 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* 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.

4) IOD lub inspektorze – należy przez to rozumieć Inspektora Ochrony Danych.
5) Kierownikach jednostek organizacyjnych – rozumie się przez to kierowników podstawowych jednostek organizacyjnych w rozumieniu niniejszej Polityki, kierowników jednostek organizacyjnych innych niż wydziały, kierowników działów administracji centralnej oraz kierowników domów studenta.
6) Kierownikach podstawowych jednostek organizacyjnych – rozumie się przez to także dyrektorów szkół doktorskich oraz dyrektora Biblioteki Uniwersyteckiej w zakresie powierzonych im obowiązków.
7) Naruszeniu ochrony danych osobowych – rozumie się przez to 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.
8) Odbiorcy danych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
9) Państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego (UE, Norwegia, Islandia, Liechtenstein).
10) Polityce – należy przez to rozumieć niniejszą Politykę bezpieczeństwa danych osobowych.
11) Procesie przetwarzania danych – należy przez to rozumieć zorganizowany i ustrukturyzowany w ramach Administratora danych proces operowania na danych osobowych w jednym wyznaczonym celu.
12) Procesorze lub Podmiocie przetwarzającym – oznacza to osobę fizyczną lub prawną, organ publiczny lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora danych.
13) Podprocesorze - oznacza to osobę fizyczną lub prawną, organ publiczny lub inny podmiot, który przetwarza dane osobowe na zlecenie procesora, ale w imieniu Administratora danych.
14) Profilowaniu – oznacza to 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.
15) Przetwarzaniu danych – rozumie się przez to, operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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.
16) Pseudonimizacji – oznacza to 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 uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

17) RODO lub rozporządzeniu – rozumie się przez to *rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).*
18) Systemie informatycznym – rozumie się przez to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej.
19) Środkach technicznych i organizacyjnych – należy przez to rozumieć wszelkie środki niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
20) Uczelni – rozumie się przez to Uniwersytet w Białymstoku.
21) Ustawie – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.
22) Zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wszelkie środki techniczne i organizacyjne zapewniające ochronę danych przed wystąpieniem zidentyfikowanych i niezidentyfikowanych możliwości wystąpienia ryzyka.
23) Zapomnieniu – rozumie się przez trwałe usuwanie, zniszczenie danych osobowych lub ich całkowitą i nieodwracalną anonimizację.
24) Zgodzie osoby, której dane dotyczą – oznacza to dobrowolne, konkretne, świadome i jednoznaczne oświadczenie woli podmiotu danych na przetwarzanie dotyczących go danych osobowych w oznaczonym celu.

2. Obowiązki Uczelni, jako Administratora danych, a także jako podmiotu przetwarzającego, wynikające z przepisów o ochronie danych osobowych w zakresie nadzoru, przestrzegania zasad, w tym w szczególności zasady prawidłowości i rozliczalności, egzekwowania praw osób, których dane dotyczą Rektor powierza:
   1) Prorektorom - w zakresie podległych jednostek i podmiotów zgodnie z określonym zakresem działania;
   2) Kanclerzowi - w zakresie podporządkowanych służbowo jednostek i podmiotów zgodnie z określonym zakresem działania;
   3) Kierownikom podstawowych jednostek organizacyjnych - w zakresie podległych jednostek oraz osób i podmiotów współpracujących, a także w zakresie doktorantów studiów doktoranckich i doktorantów szkoły doktorskiej, studentów oraz uczestników studiów podyplomowych i innych form kształcenia;
   4) Dyrektorowi Biblioteki Uniwersyteckiej - w zakresie podległej jednostki i podmiotów zgodnie z określonym zakresem działania;
   5) Administratorowi Systemów Informatycznych - w zakresie bezpieczeństwa systemów informatycznych i przydzielania dostępów do tychże systemów;
   6) Inspektorowi Ochrony Danych - w celu monitorowania przestrzegania niniejszej Polityki, przepisów RODO, identyfikowania i zgłaszania incydentów ochrony danych oraz realizacji żądań podmiotów danych.

   W zakresie jednostek podległych bezpośrednio Rektorowi oraz osób i podmiotów z nimi współpracujących nadzór pełni Rektor.
3. Dane osobowe muszą być:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub

historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

4. Uczelnia jest odpowiedzialna za przestrzeganie powyższych przepisów i wykonując swoje obowiązki dokłada wszelkich starań, aby wykazać ich przestrzeganie („rozliczalność"), w szczególności dokumentując podejmowane działania i podejmowane decyzje w zakresie ochrony danych osobowych.

Rozdział II
KATEGORIE PODMIOTÓW, KTÓRYCH DANE SĄ PRZETWARZANE W UNIWERSYTECIE W BIAŁYMSTOKU

§ 1

Uniwersytet w Białymstoku jako Administrator danych przetwarza w szczególności dane osobowe następujących kategorii osób fizycznych:

1) studentów (w tym kandydatów i członków rodzin studentów);
2) doktorantów (w tym kandydatów i członków rodzin doktorantów);
3) uczestników studiów podyplomowych i innych form kształcenia (w tym kandydatów oraz pracodawców tych uczestników);
4) osób zatrudnionych (i członków ich rodzin), w tym kandydatów do pracy;
5) zleceniobiorców, dostawców i wykonawców (w tym oferentów);
6) absolwentów;
7) autorów publikacji i recenzentów;
8) zagranicznych pracowników i zagranicznych studentów innych uczelni;
9) gości domów studenckich;
10) osób korzystających z Biblioteki Uniwersyteckiej;
11) beneficjentów grantów i projektów;
12) uczestników olimpiad, konkursów organizowanych przez Uczelnię;
13) wolontariuszy;
14) organizatorów praktyk zawodowych;
15) potencjalnych pracodawców studentów i absolwentów Uczelni;
16) dłużników i wierzycieli, w tym powodów i pozwanych w ramach spraw sądowych;
17) autorów publikacji jako stron umów wydawniczych;
18) gości Uniwersytetu.

Rozdział III
STRUKTURA ZBIORÓW DANYCH

§ 2

Administrator danych z uwzględnieniem struktury organizacyjnej Uczelni może wydzielić następujące zbiory danych, w szczególności:

1) akta osobowe pracowników;
2) zbiory informacji o kandydatach na studia, studentach, doktorantach i uczestnikach studiów podyplomowych oraz absolwentach;
3) zbiory danych zleceniobiorców;
4) wykaz delegacji służbowych;
5) ewidencja zwolnień lekarskich;
6) ewidencja pracownicza (urlopów, czasu pracy, wyjść);
7) skierowania na badania profilaktyczne;
8) listy płac pracowników;
9) deklaracje ubezpieczeniowe pracowników;
10) deklaracje i kartoteki ZUS pracowników;
11) deklaracje podatkowe pracowników;
12) dokumenty związane z pracami komisji socjalnej;
13) rejestr wypadków;
14) umowy zawierane z kontrahentami;
15) zbiór informacji o wykonawcach i dostawcach;
16) zbiory danych dotyczące praktyk studenckich;
17) zbiory danych z realizacji projektów badawczych;
18) zbiory danych z zamówień publicznych;
19) rejestr spraw sądowych;
20) zbiory informacji gromadzonych w Bibliotece Uniwersyteckiej;
21) zbiory informacji dotyczących pomocy materialnej dla studentów i doktorantów studiów doktoranckich;
22) zbiory informacji dotyczące stypendiów doktorantów szkół doktorskich;
23) zbiory z organizowanych konferencji i wydarzeń;
24) zbiory wynikające z aktów wewnątrzuczelnianych;
25) zbiory wynikające z prac komisji związków zawodowych,
26) zbiory archiwalne.

Rozdział IV
OBSZAR PRZETWARZANIA

§ 3

1. Administrator danych realizując politykę ochrony wyznacza budynki, pomieszczenia i części pomieszczeń tworzące obszar, w którym przetwarzane są dane osobowe. Obszar ten zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2. W budynkach, pomieszczeniach i częściach pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę przetwarzania i ochrony tych danych. Osoby nieposiadające upoważnienia do przetwarzania danych osobowych, w tym osoby wykonujące czynności usługowe, w szczególności takie jak: sprzątanie, remonty czy ochrona budynku, mogą przebywać w

budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wyłącznie w obecności upoważnionego przez Administratora danych pracownika lub na podstawie wydanego przez Administratora danych dokumentu zezwalającego i określającego warunki przebywania w miejscach przetwarzania danych osobowych. Zezwolenie na przebywanie w ww. pomieszczeniach i warunki przebywania mogą wynikać z umowy zawartej z podmiotem realizującym usługi.

3. W pomieszczeniach, w których znajduje się cześć ogólnodostępna oraz część, w której przetwarzane są dane osobowe, należy wyraźnie oddzielić od siebie obie części.
4. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe, może być dokonane w szczególności poprzez: montaż barierek, lady lub odpowiednie ustawienie mebli biurowych uniemożliwiające, lub co najmniej ograniczające, niekontrolowany dostęp osób niepowołanych do danych osobowych przetwarzanych w danym pomieszczeniu.
5. Stacje robocze, monitory, drukarki oraz inne urządzenia służące do przetwarzania, a zwłaszcza kopiowania danych, powinny być umiejscowione w sposób uniemożliwiający osobom nieuprawnionym podgląd informacji oraz bezpośredni i niekontrolowany dostęp.
6. W przypadku dostępu zdalnego i mobilnego do systemu informatycznego, w szczególności z użyciem sieci Internet lub radiowej sieci bezprzewodowej, w tym z użyciem prywatnych urządzeń użytkowników (w sytuacjach gdy zostało to dozwolone przez Administratora danych), administrator systemu informatycznego określa zasady korzystania, ograniczenia dostępu do systemu do niezbędnego minimum oraz technologicznego zabezpieczenia urządzeń i dostępu do systemu.
7. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, należy je zabezpieczyć przed wejściem osób niepowołanych.
8. W razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzania danych osobowych należy umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobom niepowołanym (np. w czasie nieprzekraczającym 5 minut, powinny włączać się tzw. wygaszacze ekranów).
9. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i traktowane jest jako naruszenie podstawowych obowiązków pracowniczych.
10. Dostęp do budynków i pomieszczeń Administratora danych, w których przetwarzane są dane osobowe podlega nadzorowi.
11. Nadzór polega w szczególności na: opracowaniu procedur, ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji kluczy uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz godzinę pobrania lub zdania klucza.
12. Klucze do budynków lub pomieszczeń, w których przetwarzane są dane osobowe, wydawane mogą być wyłącznie upoważnionym osobom.
13. Administrator danych realizując politykę ochrony może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
14. Szczegółowe zasady kontroli dostępu do poszczególnych obszarów (budynków, pomieszczeń), w których przetwarzane są dane osobowe określane są przez Kanclerza.

Rozdział V
ZASADA LEGALIZMU

§ 4

1. Przetwarzanie danych osobowych studentów (w tym członków rodzin studentów, kandydatów na studentów i studentów zagranicznych uczelni), organizatorów praktyk zawodowych oraz uczestników olimpiad i konkursów organizowanych przez Uczelnię jest niezbędne do przeprowadzenia procesu rekrutacyjnego, wykonania umowy, udzielania dodatkowych świadczeń nieobjętych umową, tj. np. pomocy materialnej, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt a, b, c, e, artykuł 9 ust. 2 pkt a, b RODO).
2. Przetwarzanie danych osobowych doktorantów (odpowiednio członków rodzin doktorantów, kandydatów na doktorantów, doktorantów zagranicznych uczelni) jest niezbędne do przeprowadzenia procesu rekrutacyjnego, wykonania umowy, udzielania dodatkowych świadczeń, np. pomocy materialnej, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt a, b, c, e, artykuł 9 ust. 2 pkt a, b RODO).
3. Przetwarzanie danych osobowych uczestników studiów podyplomowych (oraz kandydatów na uczestników) jest niezbędne do przeprowadzenia procesu rekrutacyjnego i wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt a, b, c, e, artykuł 9 ust. 2 pkt a, b RODO).
4. Przetwarzanie danych osobowych absolwentów jest niezbędne do wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest wymogiem w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt. c i e RODO).
5. Przetwarzanie danych osobowych pracowników i osób zatrudnionych na podstawie umów cywilnoprawnych (odpowiednio członków rodzin) jest niezbędne do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt. a, b, c, e, artykuł 9 ust. 2 pkt a, b RODO).
6. Przetwarzanie danych osobowych kandydatów na pracowników, zleceniobiorców, wykonawców jest niezbędne do przeprowadzenia procesu rekrutacyjnego (artykuł 6 ust. 1 pkt a, c RODO).
7. Przetwarzanie danych osobowych autorów i recenzentów jest niezbędne do podjęcia działań przed zawarciem umowy, a następnie do wykonania umowy i wypełnienia obowiązków prawnych ciążących na Administratorze danych (artykuł 6 ust. 1 pkt a, b, c, RODO).
8. Przetwarzanie danych osobowych pracowników zagranicznych uczelni jest niezbędne do podjęcia działań przed zawarciem umowy lub porozumienia, a następnie do wykonania umowy lub porozumienia, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt a, b, c, e RODO).
9. Przetwarzanie danych osobowych gości domów studenckich jest niezbędne do podjęcia działań przed zawarciem umowy, a następnie do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt a, b, c, e RODO).

10. Przetwarzanie danych osób korzystających z Biblioteki Uniwersyteckiej jest niezbędne do przeprowadzenia procesu rejestracyjnego, a następnie do wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt a, b, c, e RODO).
11. Przetwarzanie danych osobowych wolontariuszy przez Administratora danych jest niezbędne do podjęcia działań przed zawarciem umowy, a następnie do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt. a, b, c, e, artykuł 9 ust. 2 pkt a, b RODO).
12. Przetwarzanie danych osobowych beneficjentów grantów i projektów jest niezbędne do wykonania umowy wypełnienia, obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt. a, b, c, e, artykuł 9 ust. 2 pkt a, b RODO).
13. Przetwarzanie danych osobowych zleceniobiorców, dostawców, usługobiorców (oferentów - przyszłych dostawców, usługobiorców) jest niezbędne do przeprowadzenia negocjacji przed zawarciem umowy (artykuł 6 ust. 1 pkt. a, b RODO), a w przypadku zawarcia umowy, przetwarzanie danych osobowych jest niezbędne do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi danych (artykuł 6 ust. 1 pkt b, c, e RODO).
14. Przetwarzanie danych potencjalnych pracodawców absolwentów Uniwersytetu jest niezbędne do przeprowadzenia procesu wyboru kandydata na stanowisko pracy, a następnie do wypełnienia obowiązków prawnych ciążących na Administratorze danych jako agencji zatrudnienia (artykuł 6 ust. 1 pkt a, b, c RODO).
15. Przetwarzanie danych dłużników i wierzycieli, w tym powodów i pozwanych w ramach spraw sądowych jest oparte na przepisach prawa oraz niezbędne do obrony prawnie uzasadnionych interesów Administratora danych (artykuł 6 ust. 1 pkt c i f RODO).
16. Przetwarzanie danych autorów publikacji wydawanych przez Wydawnictwo Uniwersytetu w Białymstoku jest niezbędne do podjęcia działań przed zawarciem umowy, a następnie do wykonania umowy (artykuł 6 ust. 1 pkt b RODO).

Rozdział VI
OBOWIĄZKI ADMINISTRATORA DANYCH

§ 5

1. Administrator danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są poddawane cyklicznym przeglądom i - w razie potrzeby - uaktualnieniu.
2. Do najważniejszych obowiązków Administratora danych należy:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy,
   2) przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych,
   3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
   4) nadzór nad bezpieczeństwem danych osobowych,
   5) kontrola działań jednostek i komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami oraz postanowieniami niniejszej Polityki,

6) inicjowanie przedsięwzięć w zakresie doskonalenia systemu ochrony danych osobowych Uniwersytetu.

3. Administrator danych wyznaczył Inspektora Ochrony Danych (IOD) i przydzielił mu adres kontaktowy iod@uwb.edu.pl. Inspektor stanowi punkt kontaktowy dla podmiotów danych oraz dla Prezesa Urzędu Ochrony Danych Osobowych.
4. Administrator danych dokonał analizy i oceny rodzajów przetwarzanych danych w ramach wewnętrznych procesów oraz przeprowadził analizę ryzyka z uwzględnieniem adekwatnych, zidentyfikowanych zagrożeń, kontekstu działalności Administratora danych, zasobów i zabezpieczeń oraz opracował metodykę oceny skutków przetwarzania dla ochrony danych dla procesów wymagających przeprowadzenia takiej analizy.
5. Administrator danych opracował Procedurę postępowania w przypadku incydentu, stanowiącą Załącznik nr 1 do niniejszej Polityki.
6. Kierownicy podstawowych jednostek organizacyjnych są zobowiązani do prowadzenia w imieniu Administratora danych rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania dla procesów przetwarzania związanych z działalnością podległych im jednostek.
7. Rejestry, o których mowa w ust. 6, prowadzone są elektronicznie, przy czym lista niezbędnych informacji stanowi odpowiednio Załącznik nr 2 lub nr 3 do niniejszej Polityki.

Rozdział VII
INSPEKTOR OCHRONY DANYCH

§ 6

1. Inspektor Ochrony Danych (IOD) powoływany jest przez Administratora danych.
2. Do głównych zadań IOD należą:
   1) dbałość o zapewnienie zgodności działań Administratora danych z RODO,
   2) prowadzenie w imieniu Administratora danych rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania z zastrzeżeniem, że dane dotyczące podstawowych jednostek organizacyjnych uczelni, szkół doktorskich i Biblioteki Uniwersyteckiej są wprowadzane na podstawie przekazanych inspektorowi rejestrów prowadzonych przez właściwych kierowników,
   3) informowanie Administratora danych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i bieżące doradztwo na rzecz tych osób,
   4) monitorowanie przestrzegania RODO, innych przepisów UE lub państw członkowskich o ochronie danych oraz polityk Administratora danych lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   5) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
   6) współpraca z organem nadzorczym,
   7) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
   8) zgłaszanie incydentów do organu nadzorczego w porozumieniu z ADO,
   9) prowadzenie szkoleń pracowników Administratora danych – okresowych oraz przeprowadzanych na wniosek kierowników jednostek organizacyjnych,

10) przeprowadzanie audytów wewnętrznych, w tym kontroli podmiotów przetwarzających,
11) uczestniczenie w prowadzonych u Administratora danych wdrożeniach systemów i projektów w zakresie zadań – dbałość o spełnianie zasady domyślnej ochrony danych („privacy by design"),
12) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.

3. Administrator danych upoważnia Inspektora Ochrony Danych do:
   1) wstępu do pomieszczeń, w których przetwarzane są dane osobowe i przeprowadzenia niezbędnych sprawdzeń lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych,
   2) żądania od pracowników Administratora danych pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego (w szczególności w sytuacji zaistnienia incydentu naruszenia ochrony danych lub żądań podmiotów danych),
   3) wymagania okazania dokumentów i wszelkich danych mających bezpośredni związek z audytem,
   4) cyklicznych sprawdzeń urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.
4. Inspektor Ochrony Danych zawiadamia kierownika jednostki objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 3 dni przed dniem rozpoczęcia sprawdzenia.
5. Inspektor Ochrony Danych ma prawo dostępu do wszelkich dokumentów, urządzeń informatycznych oraz systemów związanych z przetwarzaniem danych osobowych, z wyłączeniem informacji niejawnych.
6. Po zakończeniu sprawdzenia Inspektor Ochrony Danych przygotowuje raport, który przekazywany jest Rektorowi oraz kierownikowi sprawdzanej jednostki.
7. Jeśli w ciągu 7 dni kierownik sprawdzanej jednostki nie zgłosi zastrzeżeń, uznaje się, że przyjął raport bez zastrzeżeń.
8. Rektor określa zakres realizacji zaleceń Inspektora Ochrony Danych.

Rozdział VIII
ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§ 7

1. Administrator danych wyznacza Administratorów Systemów Informatycznych (ASI), którymi są osoby odpowiedzialne za aplikacje, sprzęt oraz sieci teleinformatyczne na Uniwersytecie.
2. Do głównych zadań ASI należą:
   1) określanie zabezpieczeń elektronicznych zbiorów danych osobowych i aplikacji, za pomocą których są przetwarzane dane osobowe, i ich konsultacja z Inspektorem Ochrony Danych,
   2) monitorowanie zabezpieczeń systemów,
   3) aktualizacja systemów oraz aplikacji za pomocą których przetwarzane są dane osobowe,
   4) organizacja procesu tworzenia kopii zapasowych danych przetwarzanych w systemach informatycznych oraz oprogramowania,
   5) konfiguracja systemów kluczowych dla przetwarzanych w nich danych,
   6) przeglądy oraz konserwacja sprzętu informatycznego wykorzystywanego do przetwarzania danych osobowych,
   7) nadawanie oraz odbieranie uprawnień do systemów oraz aplikacji adekwatnie do upoważnień nadanych przez Administratora danych.

3. Szczegółowe zasady ochrony danych osobowych przetwarzanych w zbiorach informatycznych Uniwersytetu określa Instrukcja zarządzania systemem informatycznym Uniwersytetu w Białymstoku, stanowiąca Załącznik nr 2 do niniejszego Zarządzenia.

Rozdział IX
DOMYŚLNA OCHRONA DANYCH (PRIVACY BY DESIGN)

§ 8

W każdym przypadku tworzenia nowego procesu przetwarzania danych i na każdym kluczowym etapie jego projektowania i wdrażania Administrator danych uwzględnia prawa osób, których dane dotyczą, w szczególności ocenia konieczność przeprowadzania procesu oceny skutków dla ochrony danych.

Rozdział X
PROCEDURA ANALIZY RYZYKA

§ 9

1. Analizę ryzyka przeprowadza kierownik jednostki organizacyjnej w porozumieniu z Inspektorem Ochrony Danych.
2. Pracownicy Administratora danych są zobowiązani do identyfikowania i zgłaszania podatności i zagrożeń dla bezpieczeństwa danych osobowych oraz zgłaszania ich bezpośredniemu przełożonemu.
3. Analiza ryzyka jest przeprowadzana zgodnie z opracowanym planem zaakceptowanym przez Rektora i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
4. Na podstawie wyników przeprowadzonej analizy ryzyka kierownicy jednostek organizacyjnych wdrażają sposoby postępowania z ryzykiem i sygnalizują konieczność redukcji ryzyka.
5. Każdorazowo Administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.
6. Administrator danych nie może zlekceważyć ryzyka, którego wartość przekracza 6 punktów zgodnie z matrycą ryzyka stanowiącą część analizy ryzyka. Wzór udokumentowania przeprowadzenia analizy ryzyka stanowi Załącznik nr 4 do niniejszej Polityki.
7. W sytuacji, gdy ryzyko dla danego zagrożenia wynosi co najmniej 12 punktów, Administrator danych ocenia je jako wysokie i mogące skutkować naruszeniem praw i wolności podmiotów danych (osób fizycznych). W tej sytuacji Administrator danych przeprowadza ocenę skutków planowanych operacji przetwarzania dla ochrony danych. Wzór udokumentowania przeprowadzenia oceny skutków dla ochrony danych stanowi Załącznik nr 5 do niniejszej Polityki.
8. W przypadku decyzji Administratora danych o obniżeniu ryzyka Inspektor Ochrony Danych na wniosek i w porozumieniu z kierownikiem jednostki organizacyjnej (oraz ASI, jeśli dotyczy) opracowuje listę zabezpieczeń do wdrożenia oraz termin realizacji.

Rozdział XI
PROCEDURA OCENY SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH (DPIA)

§ 10

1. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadzają w imieniu Administratora danych kierownicy jednostek organizacyjnych w porozumieniu

z Inspektorem Ochrony Danych w sytuacjach, o których mowa w art. 35 RODO oraz w przypadkach wskazanych w wykazie zamieszczonym na stronie internetowej Prezesa Urzędu Ochrony Danych Osobowych (PUODO).
2. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych.
3. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz na rok w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.
4. Inspektor Ochrony Danych oraz kierownicy jednostek organizacyjnych zobligowani są do analizy konieczności przeprowadzania DPIA każdorazowo przy tworzeniu nowego procesu przetwarzania danych.

Rozdział XII
WSPÓŁPRACA Z PODMIOTAMI PRZETWARZAJĄCYMI

§ 11

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie ze wzorem oraz treścią procedury zawierania umów powierzenia. Procedura współpracy z podmiotami zewnętrznymi oraz wzór umowy powierzenia stanowi Załącznik nr 6 do niniejszej Polityki.
2. Umowa powierzenia przetwarzania danych osobowych może być zawarta nie stosując wskazanego w ust. 1 wzoru pod warunkiem, że zapisy umowy spełniają wymogi art. 28 RODO.
3. Sytuacje budzące wątpliwości powinny być konsultowane z Inspektorem Ochrony Danych.
4. O zawarciu umowy powierzenia kierownik jednostki organizacyjnej każdorazowo informuje Inspektora Ochrony Danych przesyłając na adres e-mail iod@uwb.edu.pl skan umowy. IOD prowadzi rejestr podmiotów przetwarzających dla Uczelni. Kierownicy podstawowych jednostek organizacyjnych prowadzą rejestr umów powierzenia dla podległej im jednostki.
5. Rejestr umów powierzenia, o którym mowa w ust. 4, prowadzony jest elektronicznie, przy czym lista niezbędnych informacji stanowi Załącznik nr 7 do niniejszej Polityki.
6. Przed zawarciem umowy powierzenia przetwarzania danych osobowych kierownik jednostki organizacyjnej weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej podmiotu przetwarzającego dane, która stanowi Załącznik nr 8 do niniejszej Polityki.

Rozdział XIII
PROCEDURA ZARZĄDZANIA INCYDENTAMI

§ 12

1. Każdy pracownik, który podejrzewa naruszenie ochrony danych osobowych przetwarzanych w Uniwersytecie zobowiązany jest do niezwłocznego poinformowania o tym swojego bezpośredniego przełożonego (z uwzględnieniem wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o podejrzeniu naruszenia ochrony danych osobowych), a ten do poinformowania ASI (jeśli zdarzenie dotyczy systemu informatycznego) oraz Inspektora Ochrony Danych.

2. Inspektor Ochrony Danych we współpracy z ASI (jeśli dotyczy) oraz kierownikiem jednostki, w której nastąpiło zdarzenie:
   1) przeprowadza analizę zdarzenia,
   2) stwierdza, czy nastąpiło naruszenie ochrony danych,
   3) stosownie do sytuacji rekomenduje do realizacji odpowiednie działania mające na celu zabezpieczenie przed ponownym wystąpieniem zdarzenia w przyszłości.
3. Inspektor Ochrony Danych we współpracy z ASI (jeśli dotyczy) oraz kierownikiem jednostki, w której nastąpiło zdarzenie weryfikuje, czy zgłoszone naruszenia skutkowały ryzykiem naruszenia praw lub wolności osób fizycznych.
4. Administrator danych w przypadku stwierdzenia, że naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, przy wsparciu Inspektora Ochrony Danych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.
5. Inspektor Ochrony Danych w porozumieniu z kierownikiem jednostki, w której nastąpiło zdarzenie, zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia naruszeń mogących skutkować wobec nich wysokim ryzykiem naruszenia ich praw lub wolności, chyba że zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
7. Inspektor Ochrony Danych dokumentuje naruszenia ochrony danych. Rejestr incydentów może być prowadzony elektronicznie, przy czym lista niezbędnych informacji stanowi Załącznik nr 9 do niniejszej Polityki.
8. Procedura postępowania w przypadku incydentu, do której przestrzegania zobligowani są pracownicy i inne osoby upoważnione do przetwarzania danych w imieniu Administratora danych stanowi Załącznik nr 1 do niniejszej Polityki.

Rozdział XIV
REALIZACJA PRAW OSÓB FIZYCZNYCH (PODMIOTÓW DANYCH)

§ 13

1. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, żądania skorzystania z praw przewidzianych w rozporządzeniu, Administrator danych rozpatruje indywidualnie.
2. Administrator danych niezwłocznie, nie później niż w terminie miesiąca, realizuje następujące prawa osób, których dane dotyczą:
   1) prawo dostępu do danych,
   2) prawo do sprostowania danych,
   3) prawo do usunięcia danych,
   4) prawo do ograniczenia przetwarzania danych,
   5) prawo do przenoszenia danych,
   6) prawo do sprzeciwu wobec przetwarzania danych,
   7) prawo do niepodlegania decyzjom opartym wyłącznie na profilowaniu.
3. W sytuacjach przewidzianych w art. 12 ust. 3 RODO termin ten może być wydłużony o kolejne dwa miesiące.
4. Administrator danych realizuje prawa osób fizycznych przy pomocy swoich pracowników oraz Inspektora Ochrony Danych. Kierownicy jednostek organizacyjnych zobligowani są do analizy żądania pod kątem podstaw prawnych i interesu prawnego Administratora danych oraz do udzielenia odpowiedzi na żądanie podmiotu danych. Kierownicy jednostek organizacyjnych prowadzą rejestr otrzymanych żądań zawierający w szczególności informacje o podmiocie występującym z żądaniem oraz podjętych działaniach.

5. Informacja o żądaniu podmiotu danych oraz podjętych działaniach jest przekazywana przez kierowników Inspektorowi Ochrony Danych w terminie 14 dni na adres e-mail: iod@uwb.edu.pl.
6. W przypadku realizacji praw podmiotu danych kierownik jednostki lub osoba przez niego wyznaczona niezwłocznie, nie później niż w terminie miesiąca, informuje podmiot danych o podjętych działaniach.
7. W uzasadnionych przypadkach przewidzianych w przepisach RODO Administrator danych za pośrednictwem kierownika jednostki organizacyjnej, która jest odpowiedzialna za zakres danych objętych żądaniem może odmówić realizacji praw osób, których dane dotyczą, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział XV
ODBIERANIE ZGÓD ORAZ INFORMOWANIE PODMIOTÓW DANYCH

§ 14

1. Administrator danych podaje następujące informacje każdej osobie, której dane osobowe mają być przetwarzane:
   1) adres siedziby Uniwersytetu i jego pełna nazwa,
   2) dane kontaktowe Inspektora Ochrony Danych,
   3) cele oraz podstawa prawna przetwarzania danych,
   4) prawnie uzasadnione interesy realizowane przez Uniwersytet (jeśli dotyczy), znani lub potencjalni odbiorcy danych,
   5) zamiar przekazania danych osobowych do państwa trzeciego (poza obszar Unii Europejskiej) lub organizacji międzynarodowej - gdy ma to zastosowanie,
   6) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   7) informacje o przysługujących jej prawach, w tym: prawie do żądania od Uniwersytetu dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, prawie do przenoszenia danych, prawie wniesienia skargi do organu nadzorczego (PUODO), a także prawie osoby do wycofania zgody, jeśli przetwarzanie odbywać się będzie na podstawie zgody osoby,
   8) 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 niepodania danych,
   9) informacja o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
   10) źródło pochodzenia danych osobowych, jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą oraz czy pochodzą one ze źródeł publicznie dostępnych, gdy ma to zastosowanie.
2. Informacje, o których mowa w ust. 1, należy udzielić przed uzyskaniem od osoby jej danych. Kierownicy jednostek organizacyjnych zobligowani są opracowania treści klauzul informacyjnych wykorzystywanych w związku z zakresem działań jednostki, ich aktualizację oraz zapewnienie ich należytego stosowania.
3. Jeżeli planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane zostały zebrane, przed takim dalszym przetwarzaniem należy poinformować osobę, której dane dotyczą, o tym innym celu.
4. W przypadku osób zatrudnianych na podstawie umowy o pracę (nowych pracowników) informacje określone w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uniwersytet dołączone muszą być do druku kwestionariusza osobowego.

5. W przypadku kandydatów na studia, informacje określone w ust. 1, umieszczone są na stronie rejestracji internetowego systemu rekrutacji w jego pierwszym etapie. By przejść do kolejnych etapów rejestracji, kandydat musi potwierdzić, że został o ww. okolicznościach poinformowany. Oświadczenie osoby o jej poinformowaniu przez Uniwersytet przechowywane jest w formie elektronicznej.
6. W przypadku osób zatrudnianych na podstawie umowy cywilnoprawnej informacje określone w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uniwersytet muszą być dołączone do druku umowy lub zawarte w treści umowy.
7. Treść obowiązku informacyjnego znajduje się na stronie internetowej Uniwersytetu pod adresem http://www.uwb.edu.pl/ochrona-danych-osobowych oraz może być uzyskana od IOD za pomocą adresu e-mail iod@uwb.edu.pl.
8. Pracownicy Uczelni mają obowiązek załączania treści obowiązku informacyjnego do korespondencji elektronicznej z wszystkimi odbiorcami niebędącymi pracownikami Uczelni, na przykład poprzez zamieszczenie odnośnika do adresu strony internetowej, o którym mowa w ust. 7, w stopce e-maila. Kierownik jednostki organizacyjnej może podjąć decyzję o innym sposobie spełniania obowiązku informacyjnego w podległej mu jednostce pod warunkiem, że sposób ten będzie spełniał wymogi RODO.
9. Bezwzględnie zabronione jest kopiowanie (skanowanie, kserowanie itp.) dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, jak również żądanie od osoby pozostawienia takiego dokumentu, chyba że taką możliwość przewidują przepisy prawa.
10. W przypadku utrudnionej możliwości uzyskania zgody pisemnej lub elektronicznej, gdy jest ona wymagana, uzyskuje się zgodę w formie ustnej. Zgoda w formie ustnej powinna być udokumentowana poprzez sporządzenie notatki służbowej, z podaniem: daty udzielenia zgody, imienia i nazwiska osoby, która udzieliła zgody, wykonania obowiązku poinformowania przed udzieleniem zgody o prawie do cofnięcia zgody w dowolnym momencie, treści zgody, imienia i nazwiska osoby, która otrzymała oświadczenie o zgodzie. Notatka służbowa powinna być podpisana przez osobę, która otrzymała oświadczenie o zgodzie.
11. Oświadczenie o wycofaniu zgody może być wyrażone w dowolnej formie, w tym pisemnej, elektronicznej, fax, ustnej. Cofnięcie zgody w formie ustnej powinno być udokumentowane poprzez sporządzenie notatki służbowej, z podaniem: daty cofnięcia zgody, imienia i nazwiska osoby, która cofnęła zgodę, treści cofnięcia zgody, imienia i nazwiska osoby, która otrzymała oświadczenie o cofnięciu zgody. Notatka powinna być podpisana przez osobę, która otrzymała oświadczenie o cofnięciu zgody.

Rozdział XVI
NADAWANIE I ODBIERANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 15

1. Za nadawanie i odbieranie upoważnień do przetwarzania danych osobowych odpowiada Rektor.
2. Rektor może upoważnić kierowników podstawowych jednostek organizacyjnych oraz Kanclerza Uniwersytetu do nadawania i odbierania upoważnień w podległych im jednostkach.
3. Przed dopuszczeniem do przetwarzania danych osobowych pracownik Uczelni (lub osoba współpracująca z Uczelnią) jest zobowiązany do zapoznania się z przepisami prawa dotyczącymi ochrony danych osobowych oraz zasadami ochrony danych osobowych obowiązującymi na Uniwersytecie, w szczególności z:

1) przepisami RODO oraz ustawy o ochronie danych osobowych i ich wpływu na przebieg procesów związanych z przetwarzaniem danych osobowych w Uniwersytecie,
2) zasadami wewnętrznymi obowiązującymi w Uniwersytecie, regulującymi ochronę danych osobowych, w tym treścią niniejszej Polityki oraz Instrukcją zarządzania systemem informatycznym.

4. Przed dopuszczeniem do przetwarzania danych osobowych pracownik podpisuje oświadczenie o zapoznaniu z treścią przepisów wymienionych w ust. 3. Wzór oświadczenia pracownika stanowi Załącznik nr 10 do niniejszej Polityki.
5. Przed rozpoczęciem pracy przez pracownika, którego zakres zadań obejmuje przetwarzanie danych osobowych, otrzymuje on upoważnienie odpowiednio do zakresu obowiązków, którego wzór stanowi Załącznik nr 11 do niniejszej Polityki.
6. W przypadku osoby wykonującej na podstawie umowy cywilnoprawnej usługę, w ramach której przetwarzane są dane osobowe lub osoby realizującej w Uniwersytecie praktykę zawodową, staż lub osoby w inny sposób związanej z Uniwersytetem - z wnioskiem o nadanie upoważnienia występuje bezpośredni przełożony osoby, opiekun praktyki lub stażu albo kierownik jednostki organizacyjnej zlecającej usługę lub inne zadania związane z przetwarzaniem danych osobowych.
7. Wzory upoważnień dla zleceniobiorcy, praktykanta/stażysty, w ramach procesu obsługi systemów informatycznych stanowią odpowiednio Załączniki nr 12 i 13 do niniejszej Polityki.
8. Rektor może:
   1) upoważnić osobę zgodnie z wnioskowanym zakresem,
   2) wyrazić zgodę na nadanie ograniczonych uprawnień zawierających się we wnioskowanym zakresie,
   3) nie wyrazić zgody na udzielenie upoważnienia.
9. Upoważnienie przechowywane jest w Dziale Spraw Osobowych i dołączone jest do akt pracowniczych lub - w przypadku osób innych niż pracownicy - dołączone jest do umowy o świadczenie usług, wykonanie dzieła. Kierownicy jednostek organizacyjnych przechowują kopie upoważnień podległych im pracowników.
10. Kierownik jednostki organizacyjnej jest odpowiedzialny za prowadzenie ewidencji osób upoważnionych w jednostce podległej i przekazywania takiej ewidencji Inspektorowi Ochrony Danych na każde jego żądanie. Załącznik nr 14 do niniejszej Polityki stanowi wzór ewidencji osób upoważnionych do przetwarzania danych osobowych. Ewidencja ta jest prowadzona elektronicznie.
11. Odebranie, ograniczenie lub zmiana zakresu upoważnienia do przetwarzania danych osobowych ma miejsce, gdy:
    1) z pracownikiem została rozwiązana (zakończona) umowa o pracę,
    2) zakres obowiązków służbowych pracownika uległ zmianie,
    3) osoba spowodowała swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych,
    4) istnieje uzasadniona obawa, że przetwarzanie danych osobowych przez osobę wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
12. Odebranie upoważnienia może nastąpić na wniosek: przełożonego pracownika lub zwierzchnika osoby współpracującej, ASI, IOD.

Rozdział XVII
OBOWIĄZKI KIEROWNIKÓW JEDNOSTEK ORGANIZACYJNYCH I SAMODZIELNYCH STANOWISK

§ 16

Kierownik jednostki organizacyjnej/Pracownik zatrudniony na samodzielnym stanowisku ma obowiązek w szczególności:

1) znać podstawy prawne, na jakich jednostka przez niego kierowana przetwarza dane osobowe,
2) stworzyć warunki organizacyjne i techniczne umożliwiające spełnienie wymogów wynikających z obowiązujących przepisów prawa,
3) sprawować kontrolę nad wprowadzaniem i udostępnianiem danych osobowych,
4) nadzorować zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolować przebywające w nich osoby,
5) niezwłocznie informować Inspektora Ochrony Danych (oraz ASI, jeśli dotyczy) o przypadkach naruszenia przepisów o ochronie danych osobowych.

Rozdział XVIII
POSTANOWIENIA KOŃCOWE

§ 17

1. Zasady opisane w niniejszej Polityce są przestrzegane przez pracowników, studentów i doktorantów Uniwersytetu oraz osoby upoważnione do przetwarzania danych osobowych niebędące pracownikami Uniwersytetu ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako naruszenie obowiązków pracowniczych.
3. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz także ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych.*

Załącznik nr 1
do Polityki bezpieczeństwa
danych osobowych

Procedura postępowania w przypadku incydentu

1. Celem procedury jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz unikanie ryzyka występowania zagrożeń i incydentów naruszenia bezpieczeństwa w przyszłości.
2. Każdy pracownik i współpracownik upoważniony do przetwarzania danych osobowych zobowiązany jest do niezwłocznego powiadamiania bezpośredniego przełożonego o stwierdzeniu podatności lub wystąpieniu incydentu.
3. Do typowych podatności i zagrożeń dla bezpieczeństwa danych osobowych, na które należy zwrócić uwagę, należą:
   1) niezabezpieczenie albo niewłaściwe zabezpieczenie sprzętu lub oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   2) nieprawidłowe zabezpieczenie pomieszczeń, urządzeń i dokumentów;
   3) lekceważenie i nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (w szczególności: niestosowanie zasady czystego ekranu, polityki kluczy, polityki czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
4. Kierownicy jednostek organizacyjnych są zobowiązani do zapewnienia wdrożenia odpowiednich środków organizacyjnych mających na celu minimalizację wystąpienia zagrożenia dla bezpieczeństwa danych osobowych.
5. Do incydentów ochrony danych, których podejrzenie należy zgłosić, należą w szczególności:
   1) brak możliwości dostępu do danych np. zapomnienie hasła, zagubiony klucz do pomieszczenia lub mebli biurowych, w których przechowywane są dokumenty,
   2) poruszanie się po obszarze przetwarzania danych nieznanych, niezidentyfikowanych osób,
   3) zniszczony mebel, w którym przechowywanie są dokumenty, brak nośników informacji,
   4) zalane pomieszczenie,
   5) zmodyfikowana postać przetwarzanych danych związanych z niepoprawną ich treścią,
   6) usiłowanie lub fakt nieuprawnionego dostępu do danych lub pomieszczenia, w którym dane są przetwarzane,
   7) zniszczenie lub próby zniszczenia danych,
   8) odmienne funkcjonowanie systemu informatycznego, a w szczególności budzące wątpliwości wyświetlane komunikaty i informacje o błędach oraz nieprawidłowościach w wykonywaniu operacji, zmieniony wygląd oprogramowania systemu,
   9) utrata danych,
   10) złośliwe oprogramowanie, ataki hakerskie i inne próby nielegalnego logowania się do systemu lub włamania do systemu.
6. Każdy pracownik, który podejrzewa naruszenie ochrony danych osobowych przetwarzanych w Uniwersytecie zobowiązany jest do niezwłocznego poinformowania o tym swojego bezpośredniego przełożonego (z uwzględnieniem wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji podejrzenia naruszenia ochrony danych osobowych), a ten do poinformowania ASI (jeśli zdarzenie dotyczy systemu informatycznego) oraz Inspektora Ochrony Danych.

7. Inspektor Ochrony Danych we współpracy z ASI (jeśli dotyczy) oraz kierownikiem jednostki, w której nastąpiło zdarzenie:
   1) przeprowadza analizę zdarzenia,
   2) stwierdza, czy nastąpiło naruszenie ochrony danych,
   3) stosownie do sytuacji rekomenduje do realizacji odpowiednie działania mające na celu zabezpieczenie przed ponownym wystąpieniem zdarzenia w przyszłości.
8. Inspektor Ochrony Danych we współpracy z ASI (jeśli dotyczy) oraz kierownikiem jednostki, w której nastąpiło zdarzenie weryfikuje, czy zgłoszone naruszenia skutkowały ryzykiem naruszenia praw lub wolności osób fizycznych.
9. Administrator danych w przypadku stwierdzenia, że naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, przy wsparciu Inspektora Ochrony Danych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.
10. Inspektor Ochrony Danych w porozumieniu z kierownikiem jednostki, w której nastąpiło zdarzenie, zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia naruszeń mogących skutkować wobec nich wysokim ryzykiem naruszenia ich praw lub wolności, chyba że zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
11. Inspektor Ochrony Danych dokumentuje naruszenia ochrony danych.

Załącznik nr 2
do Polityki bezpieczeństwa
danych osobowych

Wzór rejestru czynności przetwarzania[1]

Nazwa procesu	
Właściciele procesu (jednostki)	
Cel przetwarzania	
Podstawa prawna przetwarzania	
Kategorie osób, których dane dotyczą	
Zakres danych przetwarzanych w procesie	
Odbiorcy danych lub kategorie odbiorców danych	
Przekazywanie danych do państwa trzeciego	
Planowany termin usunięcia danych	
Opis zabezpieczeń technicznych	
Opis zabezpieczeń organizacyjnych	

[1] Wzór zawiera wykaz niezbędnych informacji. Rejestr prowadzony jest elektronicznie.

Załącznik nr 3
do Polityki bezpieczeństwa
danych osobowych

Wzór rejestru kategorii czynności przetwarzania[1]

Kategoria czynności przetwarzania	
Opis zabezpieczeń technicznych i organizacyjnych (jeśli dotyczy)	
Nazwa i dane kontaktowe administratora danych lub współadministratorów danych, ich przedstawicieli i inspektora ochrony danych (jeśli dotyczy)	
Okres powierzenia przetwarzania danych	
Przekazywanie danych do państwa trzeciego i opis zabezpieczeń przekazywania (jeśli dotyczy)	
Podpowierzenie danych – nazwa podmiotu, któremu podpowierzono dane i kategorie podpowierzonych czynności przetwarzania	

[1] Wzór zawiera wykaz niezbędnych informacji. Rejestr prowadzony jest elektronicznie.

Załącznik nr 4
do Polityki bezpieczeństwa
danych osobowych

Wzór udokumentowania przeprowadzenia analizy ryzyka

Analiza ryzyka dla naruszenia praw i wolności osób fizycznych z uwzględnieniem zidentyfikowanych zagrożeń i podatności

Zidentyfikowane zagrożenie	Podatności	Skutek dla Administratora danych związany z pojawieniem się incydentu (S)	Zabezpieczenia minimalizujące prawdopodobieństwo wystąpienia incydentu	Prawdopodobieństwo wystąpienia incydentu (P)	Ryzyko (S x P)	Plan postępowania z ryzykiem

Stosowana matryca ryzyka

1. Tabela przyjętych wartości S (Skutek dla Administratora danych związany z pojawieniem się incydentu)

Ocena	Znaczenie	
1	Mały	Nieznaczne utrudnienia w funkcjonowaniu Administratora danych i znikome skutki dla praw i wolności podmiotów danych.
2	Średni	Zauważalne utrudnienia w systemie bezpieczeństwa informacji, w tym w obszarze praw i wolności podmiotów danych.
3	Duży	Znaczne utrudnienia w systemie bezpieczeństwa informacji, czego wynikiem może być szkoda po stronie podmiotów danych.
4	Bardzo duży	Zagrożenie wywołuje bardzo znaczące straty, w tym szkody po stronie podmiotów danych.

2. Tabela przyjętych wartości P (Prawdopodobieństwo wystąpienia incydentu)

Ocena	Poziom prawdopodobieństwa	Charakterystyka
1	Bardzo rzadko	Zdarzenie 1 raz na 10 lat
2	Rzadko	Zdarzenie 1 raz na 5 lat
3	Często	Zdarzenie 1 raz 3 miesiące
4	Bardzo często	Zdarzenie 1 raz na 2 tygodnie

Załącznik nr 5
do Polityki bezpieczeństwa
danych osobowych

Wzór udokumentowania przeprowadzenia oceny skutków dla ochrony danych

Ocena skutków dla ochrony danych

Identyfikacja czynności w procesie i powiązań	Nazwa procesu	
	Właściciel procesu	
	Cel procesu	
	Opis procesu i czynności realizowanych w ramach procesu	
Analiza niezbędności DPIA zgodnie z art. 35 RODO	Czy realizacja procesu może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? Czy operacja przetwarzania została ujęta w wykazie publikowanym przez organ nadzorczy?	
	Systematyczna, kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną	
	Przetwarzanie na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych	

	dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO		
	Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie		
	Ewaluacja lub ocena, w tym profilowanie i przewidywanie, szczególnie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motywy 71 i 91 RODO)		
	Przetwarzanie mające na celu podejmowanie decyzji dotyczących osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej" lub „w podobny sposób znacząco wpływających na osobę fizyczną" (art. 35 ust. 3 lit. a RODO).		
	Dokonano porównania lub połączenia zestawów danych		
	Dane dotyczące osób wymagających szczególnej opieki		
	Transgraniczne przekazywanie danych poza Unię Europejską		
Ocena niezbędności i proporcjonalności	Środki wpływające na	Konkretny, wyraźny i prawnie uzasadniony cel	

	niezbędność i proporcjonalność przetwarzania	Zgodność przetwarzania z prawem	
		Dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów	
		Ograniczenie okresu przechowywania	
	Środki przyczyniające się do realizacji praw osób, których dane dotyczą	Informacje udzielone osobie, której dane dotyczą	
		Prawo dostępu i przenoszenia danych	
		Prawo do sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu	
		Zabezpieczenia dotyczące przekazywania danych	
		Uprzednie konsultacje	
Czy doszło do działań niepożądanych w ramach danych w procesie?	Niezgodne z prawem zniszczenie		
	Przypadkowe zniszczenie		
	Nieuprawniony dostęp		

	Utracenie	
	Nieuprawnione zmodyfikowanie	
	Nieuprawnione ujawnienie	
Prawdopodobieństwo	Kiedy ostatni raz doszło do zdarzenia?	
Skutek wystąpienia zdarzenia dla osoby fizycznej	Dyskryminacja	
	Kradzież tożsamości lub oszustwo dotyczące tożsamości	
	Strata finansowa	
	Naruszenie dobrego imienia	
	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową	
	Nieuprawnione odwrócenie pseudonimizacji	
	Wszelka inna znacząca szkoda gospodarcza lub społeczna	

Środki planowane w celu zaradzenia ryzyku	

Załącznik nr 6
do Polityki bezpieczeństwa
danych osobowych

Procedura współpracy z podmiotami zewnętrznymi oraz wzór umowy powierzenia

1. W przypadku współpracy z zewnętrznym podmiotem każdorazowo należy rozważyć, czy dochodzi do powierzenia przetwarzania danych. Istotne jest, czy taki podmiot uzyskuje dostęp do danych, których Administratorem danych jest Uniwersytet, w postaci dostępu do baz danych, systemów, dokumentów oraz czy gwarantuje przy tym Uniwersytetowi standardy bezpieczeństwa, o jakich mowa w art. 28 i 32 RODO.
2. Ocena, czy dany podmiot współpracujący uzyskuje dostęp do danych polegający na powierzeniu danych spoczywa na osobie upoważnionej do zawarcia umowy. Jeśli na podstawie treści umowy osoba upoważniona przez Rektora do zawarcia danej umowy oceni, że zachodzi powierzenie danych, podejmuje decyzję o zawarciu dodatkowej umowy zgodnie z wzorem określonym w niniejszym Załączniku.
3. Umowa powierzenia może być zawarta bez korzystania z określonego w niniejszym Załączniku wzoru pod warunkiem, że treść zapisów będzie zgodna z art. 28 RODO.
4. W przypadku istotnych wątpliwości warunki powierzenia przetwarzania danych osobowych powinny być skonsultowane z Inspektorem Ochrony Danych.
5. Kierownicy jednostek organizacyjnych zobligowani są do prowadzenia ewidencji podmiotów przetwarzających z uwzględnieniem następujących informacji: nazwa procesora, numer i data zawarcia umowy powierzenia, kategoria osób których dane dotyczą, kategoria danych osobowych, zakres przetwarzanych danych, zakres czynności przetwarzania.
6. Ewidencja podmiotów przetwarzających powinna być przekazywana Inspektorowi Ochrony Danych nie rzadziej niż dwa razy w roku oraz na każdorazowe żądanie Inspektora Ochrony Danych.
7. Inspektor Ochrony Danych może w imieniu Administratora danych weryfikować zgodność z ogólnym rozporządzeniem o ochronie danych oraz zawartymi umowami powierzenia wszystkich podmiotów przetwarzających.

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia .....w Białymstoku

pomiędzy:

Uniwersytetem w Białymstoku, ul. Świerkowa 20 B, 15-328 Białystok
zwanym dalej **Zleceniodawcą** lub **Administratorem danych**

reprezentowanym przez

.....

a

.....
zwanym dalej **Wykonawcą** lub **Podmiotem Przetwarzającym**

§ 1

Powierzenie przetwarzania danych osobowych

1. Zleceniodawca powierza Wykonawcy w zgodzie z brzmieniem art. 28 *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 (dalej jako RODO)* dane osobowe następujących kategorii osób:
   .....
   .....
2. Zleceniodawca oświadcza, że jest Administratorem danych, które powierza Wykonawcy do przetwarzania.
3. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w niniejszej umowie.

§ 2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał powierzone dane osobowe dotyczące kategorii osób wymienionych w § 1 ust. 1 wyłącznie w związku z wykonywaniem obowiązków wynikających z Umowy .....
2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę jedynie przez czas obowiązywania Umowy, o której mowa w ust.1.

§ 3

Sposób wykonania umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 28 RODO, tj. w szczególności:
   1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora danych;
   2) zapewnia, by osoby upoważnione przez niego do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;

3) podejmuje wszelkie adekwatne środki wymagane na mocy art. 32 RODO, w tym zabezpiecza dane przed nieuprawnionym udostępnieniem;

4) przestrzega warunki korzystania z usług innego podmiotu przetwarzającego, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO (tj. prawa do bycia zapomnianym, przenoszalności danych, wniesienia sprzeciwu itp.);

5) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi danych wywiązać się z obowiązków określonych w art. 32–36 RODO;

6) po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi danych dane osobowe;

7) udostępnia Administratorowi danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków oraz umożliwia mu lub audytorowi upoważnionemu przez Administratora danych przeprowadzanie audytów, w tym inspekcji w zakresie zgodności przetwarzania z umową oraz RODO;

8) informuje Administratora danych o jakiejkolwiek kontroli organu nadzorczego w zakresie powierzonych danych osobowych;

9) niezwłocznie, nie później niż w terminie 24 godzin od zaistnienia zdarzenia, informuje Administratora danych o wszelkich incydentach bezpieczeństwa danych osobowych mających wpływ na prawa i wolności podmiotów danych. Zgłoszenia należy dokonać na adres – iod@uwb.edu.pl.

2. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie po uzyskaniu uprzedniej pisemnej zgody Zleceniodawcy, z zachowaniem gwarancji wynikających z art. 28 RODO.

§ 4

Odpowiedzialność Wykonawcy

Wykonawca jest odpowiedzialny w szczególności za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, w tym za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym. Z tego tytułu ponosi odpowiedzialność odszkodowawczą względem Zleceniodawcy.

§ 5

Czas obowiązywania umowy

1. Niniejsza umowa w zakresie przetwarzania danych obowiązuje od dnia zawarcia, przez cały czas obowiązywania Umowy, o której mowa w § 2 ust. 1.
2. Administrator danych może wypowiedzieć Wykonawcy umowę w trybie natychmiastowym i odmówić dostępu do danych w przypadku niewywiązywania się z postanowień niniejszej Umowy.

§ 6

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Zleceniodawcy i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki techniczne wykorzystywane do odbioru, przekazywania oraz przechowywania danych osobowych (poczta elektroniczna, telefon) gwarantowały zabezpieczenie danych poufnych przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

_____ _____

(Administrator danych) *(Podmiot przetwarzający)*

Załącznik nr 7
do Polityki bezpieczeństwa
danych osobowych

Wzór rejestru umów powierzenia[1]

Nazwa procesora	Numer i data zawarcia umowy powierzenia	Kategoria osób, których dane dotyczą, kategoria danych osobowych, zakres przetwarzanych danych, zakres czynności przetwarzania

[1] Wzór zawiera wykaz niezbędnych informacji. Rejestr prowadzony jest elektronicznie.

Załącznik nr 8
do Polityki bezpieczeństwa
danych osobowych

Lista kontrolna podmiotu przetwarzającego dane

Weryfikacja zgodności podmiotu przetwarzającego dane z ogólnym rozporządzeniem o ochronie danych

Nazwa podmiotu przetwarzającego:

Przepis prawa	Opis wymogu	Stopień zgodności	Uwagi	Rekomendacje
Art. 28 RODO	Czy podmiot przetwarzający spełnia wymogi RODO?			
	Czy podmiot przetwarzający na bieżąco informuje o zmianie sposobu przetwarzania powierzonych danych?			
	Czy podmiot przetwarzający korzysta z podprocesora przy przetwarzaniu powierzonych danych osobowych?			
	Czy z podmiotem przetwarzającym doszło do zawarcia pisemnej umowy?			
	Czy umowa z podmiotem przetwarzającym zawiera zakres powierzonych danych?			
	Czy umowa z podmiotem przetwarzającym zawiera czas trwania przetwarzania?			
	Czy umowa z podmiotem przetwarzającym zawiera opis charakteru przetwarzania i cele przetwarzania?			

	Czy umowa z podmiotem przetwarzającym zawiera opis rodzaju danych oraz kategorię osób, których dane dotyczą?			
	Czy umowa z podmiotem przetwarzającym zawiera obowiązki i uprawnienia Administratora danych?			
	Czy podmiot przetwarzający zapewnia, by przetwarzanie odbywało się na udokumentowane polecenie Administratora danych?			
	Czy podmiot przetwarzający zapewnia poufność danych?			
	Czy podmiot przetwarzający pomaga Administratorowi danych w relacjach z osobą, której dane dotyczą?			
	Czy podmiot przetwarzający usuwa lub zwraca powierzone dane po zakończeniu przetwarzania?			
	Czy podmiot przetwarzający umożliwia kontrole bezpośrednie z ramienia Administratora danych?			
	Czy podmiot przetwarzający informuje Administratora danych, gdy jego polecenia naruszają RODO?			
	Czy podmiot przetwarzający odpowiada za zgodne z prawem przetwarzanie danych przez podwykonawców?			
	Czy podmiot przetwarzający realizuje obowiązek nadawania upoważnień do przetwarzania danych osobowych?			

Art. 30 RODO	Czy podmiot przetwarzający realizuje obowiązek prowadzenia rejestru kategorii czynności przetwarzania?			
Art. 32 RODO	Czy podmiot przetwarzający stosuje pseudonimizację lub szyfrowanie powierzonych danych?			
	Czy podmiot przetwarzający posiada zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania powierzonych danych?			
	Czy podmiot przetwarzający posiada zdolność do szybkiego przywrócenia dostępności danych w razie incydentu?			
	Czy podmiot przetwarzający prowadzi regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych zabezpieczeń?			
	Czy podmiot przetwarzający uwzględnia następujące ryzyka wynikające z przypadkowego lub niezgodnego z prawem: - zniszczenia, - utraty, - modyfikacji, - nieuprawnionego ujawnienia lub dostępu do danych?			
Art. 33 RODO	Czy podmiot przetwarzający zgłasza naruszenia ochrony danych Administratorowi danych?			
Art. 37 RODO	Czy podmiot przetwarzający wyznaczył Inspektora Ochrony Danych?			

Art. 46 RODO	Czy podmiot przetwarzający przekazuje powierzone dane do państwa trzeciego?			

Załącznik nr 9
do Polityki bezpieczeństwa
danych osobowych

Wzór rejestru incydentów[1]

Opis okoliczności wystąpienia incydentu	Skutki naruszenia	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba lub jednostka odpowiedzialna za wdrożenie działań naprawczych	Konieczność poinformowania organu nadzorczego i podmiotu danych

[1] Wzór zawiera wykaz niezbędnych informacji

Załącznik nr 10
do Polityki bezpieczeństwa
danych osobowych

Białystok, dnia .....

OŚWIADCZENIE PRACOWNIKA O ZAPOZNANIU SIĘ Z PRZEPISAMI DOTYCZĄCYMI OCHRONY DANYCH OSOBOWYCH

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (RODO) oraz wewnętrznymi procedurami w tym zakresie.

Zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w upoważnieniu do przetwarzania danych lub obowiązkach służbowych na zajmowanym stanowisku,
- zachowania w tajemnicy powierzonych danych osobowych oraz sposobów zabezpieczenia danych,
- zapobiegania incydentom z zakresu ochrony danych osobowych takim jak np. przypadkowe lub niezgodne z prawem zniszczenie, utrata, modyfikacja danych osobowych, nieuprawnione ujawnienie, nieuprawniony dostęp do danych osobowych.

Zostałem przeszkolony i poinformowany o konsekwencjach naruszenia przepisów ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

.....
(podpis)

Pracodawca przekazał mi wszystkie elementy obowiązku informacyjnego, o których mowa w art. 13 ust. 1 i ust. 2 RODO, w tym m.in. kto jest Administratorem moich danych, w jakim celu są przetwarzane, przez jaki czas będą przechowywane oraz jakie mam prawa wynikające z przetwarzania moich danych przez pracodawcę jako Administratora danych.

.....
(podpis)

Załącznik nr 11
do Polityki bezpieczeństwa
danych osobowych

Białystok, dnia..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 i art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* niniejszym upoważniam:

_____

(imię, nazwisko)

_____

(jednostka organizacyjna)

do przetwarzania danych osobowych w zakresie:

.....

.....

.....

Pracownik będzie wykonywał obowiązki związane z przetwarzaniem danych osobowych zgodnie z poleceniami Administratora danych.

Upoważnienie obowiązuje przez okres zatrudnienia. Pracownik jest zobowiązany do zachowania poufności zarówno w trakcie, jak i po wygaśnięciu upoważnienia oraz do przestrzegania zasad i procedur ochrony danych osobowych obowiązujących w Uniwersytecie w Białymstoku.

_____

(podpis Rektora lub osoby upoważnionej)

Upoważnienie odebrałem(-am):

....

(data) *(podpis)*

Załącznik nr 12
do Polityki bezpieczeństwa
danych osobowych

Białystok, dnia ..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 i art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* niniejszym upoważniam:

_____

(imię, nazwisko)

do przetwarzania danych osobowych w zakresie:

.....

.....

..... .

Zleceniobiorca/stażysta/praktykant[1] będzie wykonywał obowiązki związane z przetwarzaniem danych osobowych zgodnie z poleceniami Administratora danych.

Upoważnienie obowiązuje przez okres współpracy w ramach umowy ..... . Zleceniobiorca/stażysta/praktykant[1] jest zobowiązany do zachowania poufności zarówno w trakcie, jak i po wygaśnięciu upoważnienia oraz do przestrzegania zasad i procedur ochrony danych osobowych obowiązujących w Uniwersytecie w Białymstoku.

_____

(podpis Rektora lub osoby upoważnionej)

Upoważnienie odebrałem:

....

(data) *(podpis)*

[1] niepotrzebne skreślić

Załącznik nr 13
do Polityki bezpieczeństwa
danych osobowych

Białystok, dnia ..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

w ramach procesu obsługi systemów informatycznych

Na podstawie art. 29 i art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* niniejszym upoważniam:

_____

(imię, nazwisko)

_____

(jednostka organizacyjna)

do przetwarzania danych osobowych znajdujących się w zbiorach danych wszystkich systemów informatycznych/w następujących systemach informatycznych[1]:

.....
.....
..... .

Pracownik będzie przetwarzał dane osobowe wyłącznie w celu wykonywania obowiązków służbowych związanych z zajmowanym stanowiskiem - zgodnie z poleceniami Administratora danych.

Upoważnienie obowiązuje na cały okres zatrudnienia na Uniwersytecie w Białymstoku. Pracownik jest zobligowany do zachowania poufności także po wygaśnięciu niniejszego upoważnienia oraz do przetwarzania zasad i procedur ochrony danych osobowych obowiązujących w Uniwersytecie w Białymstoku.

_____

(podpis Rektora lub osoby upoważnionej)

Upoważnienie odebrałem:

....
(data) *(podpis)*

[1] niepotrzebne skreślić

Załącznik nr 14
do Polityki bezpieczeństwa
danych osobowych

WZÓR EWIDENCJI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH[1]

Zakres upoważnienia		Imię i nazwisko użytkownika	Identyfikator użytkownika w systemie (jeśli przyznano)	Data nadania upoważnienia	Data ustania upoważnienia
Nazwa procesu, w tym zidentyfikowanych zbiorów	Rodzaj uprawnień				

[1] Ewidencja prowadzona jest elektronicznie.