Zachodniopomorska
Szkoła Biznesu
w Szczecinie

ul. Żołnierska 53, 71-210 Szczecin
tel. (+48 91) 814 94 10
fax (+48 91) 814 94 40
www.zpsb.szczecin.pl

# POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W ZACHODNIOPOMORSKIEJ SZKOLE BIZNESU W SZCZECINIE

## Spis treści

## 1. Podstawa prawna

1. Niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych, zwana dalej **Polityką** została opracowana przez Zachodniopomorską Szkołę Biznesu w Szczecinie, zwaną dalej **Uczelnią** z uwzględnieniem następujących przepisów:
    a. Prawo o szkolnictwie wyższym i nauce, zwane dalej **Prawem**;
    b. 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) (Dz. Urz. UE L z 4.05.2016, str. 1-88), zwane dalej **RODO**;
    c. Ustawy o ochronie danych osobowych, zwanej dalej **Ustawą**.

## 2. Słownik pojęć

1. **dane osobowe** - 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. **dane biometryczne** – 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. **przetwarzanie** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;
4. **profilowanie** - dowolna forma zautomatyzowanego przetwarzania danych osobowych w celu ich wykorzystania 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;
5. **zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którą osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego;
6. **naruszenie ochrony danych osobowych** - 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;
7. **Administrator Danych (ADO)** - Uczelnia reprezentowana przez Rektora;
8. **Pełnomocnik Danych (PDO)** – Pełnomocnik Rektora ds. Danych Osobowych, któremu Administrator Danych Osobowych powierzył nadzorowanie i koordynowanie zasad postępowania przy przetwarzaniu danych osobowych w Uczelni;
9. **Lokalny Administrator Danych (LADO)** – osoba, której przekazano obowiązki i uprawnienia Administratora Danych Osobowych;
10. **Administrator Systemu Informatycznego (ASI)**–pracownik obsługujący system informatyczny i/lub nadzorujący jego pracę, odpowiadający za jego funkcjonowanie i bezpieczeństwo, w szczególności funkcjonowanie i bezpieczeństwo sieci komputerowej i serwerów, w których przetwarzane są dane osobowe;
11. **podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
12. **odbiorca danych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a RODO (chodzi o przedstawiciela w Rzeczypospolitej Polskiej wyznaczonego przez administratora danych spoza UE), podmiotu, o którym mowa w art. 31 RODO (chodzi o procesora), organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

13. **jednostka** - jednostka organizacyjną Uczelni;
14. **system informatyczny** - zespół współpracujących ze sobą urządzeń tworzących sieć komputerową, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
15. **obszar przetwarzania** - budynki, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe, zabezpieczony przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

## 3. Cel i zakres Polityki

1. Polityka określa zasady postępowania, stosowane środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych przetwarzanych w formie papierowej oraz w systemach informatycznych.
2. Uczelnia realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:
   a) zbierane i przetwarzane zgodnie z prawem, w sposób przejrzysty i rzetelny,
   b) zbierane i przetwarzane tylko w konkretnych, uzasadnionych i zgodnych z prawem celach,
   c) merytorycznie poprawne, o minimalnym zakresie niezbędnym do celów zbierania i przetwarzania,
   d) przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą,
   e) przetwarzane w okresie nie dłuższym niż wymagany celem przetwarzania,
   f) chronione przed niedozwolonym czy niezgodnym z prawem przetwarzaniem; utratą danych, zniszczeniem lub uszkodzeniem,
   g) rozliczalne, czyli przetwarzane zgodnie z zasadami wymienionymi powyżej.
3. Uczelnia w sposób ciągły doskonali środki fizyczne, informatyczne i organizacyjne, zabezpieczające dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Uczelnia realizując cele polityki zapewnia: szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony, bieżącą identyfikację i szacowanie ryzyka w zapewnieniu bezpieczeństwa danych osobowych oraz ciągłe monitorowanie skuteczności zastosowanych rozwiązań zabezpieczających dane osobowe.
5. Szczegółowe zasady ochrony danych osobowych przetwarzanych w zbiorach informatycznych Uczelni określa Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych stanowiąca załącznik nr 1.
6. Niniejsza Polityka obowiązuje wszystkich pracowników i współpracowników Uczelni przetwarzających dane osobowe lub mających dostęp do danych.
7. Pracownicy uczelni i współpracownicy, studenci, słuchacze studiów podyplomowych, uczestnicy kursów i szkoleń oraz inne osoby, których dane są przetwarzane w jednostkach organizacyjnych Uczelni, mają prawo do: ochrony danych ich dotyczących, kontroli zasad ich zbierania i przetwarzania, do poprawiania lub usunięcia, wycofania zgody, zgłoszenia sprzeciwu lub żądania ograniczenia przetwarzania, udostępnienia i przeniesienia, jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.
8. Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych.
9. Sprawy sporne związane z ochroną danych osobowych rozstrzyga Rektor

## 4. Osoby odpowiedzialne za przetwarzanie danych osobowych

1. Uczelnia jest ADO w rozumieniu art. 4 pkt 7 RODO.
2. Wobec innych administratorów, którzy powierzyli Uczelni dane do przetwarzania, Uczelnia jest podmiotem przetwarzającym.
3. W imieniu ADO w sprawach przetwarzania danych osobowych wszelki czynności wykonuje i decyzje podejmuje Rektor, zgodnie z obowiązującymi przepisami w zakresie ochrony danych osobowych.
4. Uczelnia zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. Dane osobowe mogą przetwarzać wyłącznie osoby posiadające właściwe upoważnienie.

6. Rektor zobowiązuje do przestrzegania przepisów prawa oraz zasad dotyczących przetwarzania danych osobowych wszystkich pracowników, współpracowników, studentów (w zakresie pełnienia funkcji związanych z działalnością Uczelni, w tym funkcji samorządowych) oraz osoby i podmiotach współpracujących, biorących udział w czynnościach przetwarzania danych osobowych.
7. Rektor zobowiązuje wszystkich pracowników do zgłaszania POD zauważonych nieprawidłowości lub naruszeń zasad ochrony danych osobowych.
8. Rektor powołuje się Pełnomocnika Rektora ds. Danych Osobowych w Uczelni (PDO).
9. PDO podlega bezpośrednio Rektorowi.
10. PDO jest upoważniony do przetwarzania danych osobowych w zakresie niezbędnym do pełnienia swej funkcji oraz zobowiązany do zachowania tajemnicy tych danych.
11. Zadaniem PDO jest nadzorowanie i koordynowanie w Uczelni zasad postępowania przy przetwarzaniu danych osobowych, a w szczególności:
    a) monitorowanie przestrzegania przez pracowników upoważnionych do przetwarzania danych osobowych zapisów niniejszej Polityki oraz przepisów prawa i aktów wewnętrznych dotyczących ochrony danych osobowych;
    b) informowanie ADO, LADO, ASI, pracowników przetwarzających dane osobowe oraz podmiotów przetwarzających o obowiązkach spoczywających na nich na mocy przepisów prawa oraz aktów wewnętrznych dotyczących ochrony danych osobowych, a także doradzanie im w tych sprawach;
    c) monitorowanie skuteczności środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w Uczelni, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem;
    d) sprawowanie stałej kontroli nad zgodnością procesów przetwarzania danych z zasadami wynikającymi z obowiązujących przepisów prawa;
    e) klasyfikowanie zbiorów danych osobowych przetwarzanych w Uczelni;
    f) rejestrowanie zbiorów danych o ile wymagają tego przepisy;
    g) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
    h) udzielanie na żądanie ADO, LADO, ASI zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej realizacji;
    i) wnioskowanie o usunięcie uchybień w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych wraz z przedstawieniem propozycji rozwiązań zmierzających do usunięcia naruszeń;
    j) prowadzenie ewidencji miejsc przetwarzania danych osobowych i sposobu ich zabezpieczenia;
    k) prowadzenie ewidencji wniosków o udostępnianie danych osobowych instytucjom i osobom spoza Uczelni wg wzoru w załączniku nr 14;
    l) prowadzenie rejestru czynności przetwarzania danych osobowych, stanowiącego załącznik nr 2;
    m) prowadzenie rejestru kategorii czynności przetwarzania danych osobowych w imieniu administratora, stanowiącego załącznik nr 3;
    n) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, załącznik nr 4;
    o) prowadzenie rejestru naruszeń ochrony danych osobowych, Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych załącznik nr 5;
    p) kontrola uzupełnienia zakresów czynności osób zatrudnionych przy przetwarzaniu danych o obowiązki wynikające z ustawy;
    q) kontrola przekazywania przez LADO zewidencjonowanych upoważnień do przetwarzania danych osobowych (załącznik nr 8) do Kadr w celu włączenia ich do akt osobowych pracowników;
    r) opracowywanie oraz opiniowanie projektów, zarządzeń i innych dokumentów, w zakresie dotyczącym danych osobowych;
    s) organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania danych osobowych;
    t) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych;
    u) identyfikowanie i analizowanie zagrożenia i ryzyka, na które może być narażone przetwarzanie danych osobowych;
    v) wnioskowanie do ADO o wdrożenie określonych zabezpieczeń adekwatnych do zagrożeń i ryzyka;
    w) wydawanie poleceń pracownikom ADO przetwarzającym dane osobowe w zakresie stosowania określonych zabezpieczeń procesu przetwarzania danych;
    x) okresowe wstrzymywanie przetwarzania danych osobowych w przypadku naruszenia ich bezpieczeństwa skutkującego wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą;

y) konsultowanie w imieniu ADO z organem nadzorującym kwestie związane z wysokim ryzykiem przetwarzania zgodnie z art. 36 RODO, a także prowadzenie stosownych konsultacji we wszelkich innych sprawach;
z) udzielanie informacji dotyczących przetwarzania osobom, których dane przetwarzane są w Uczelni.

12. Obowiązki wynikające z ustawy o ochronie danych osobowych Rektor, jako ADO przekazuje LADO, którymi są:
    a) Prorektor ds. nauczania w zakresie podległych pracowników i jednostek oraz osób i podmiotów współpracujących;
    b) Prorektor ds. Rozwoju w zakresie podległych pracowników i jednostek, oraz słuchaczy i osób uczestniczących w innych formach kształcenia oraz osób i podmiotów współpracujących;
    c) Dziekani w zakresie podległych pracowników i jednostek, studentów, słuchaczy i osób uczestniczących w innych formach kształcenia oraz osób i podmiotów współpracujących;
    d) Kanclerz w zakresie pracowników podległych jednostek oraz osób i podmiotów współpracujących;
    e) Menedżerowie projektów w zakresie jednostek i osób jemu podległych w ramach realizacji projektu oraz osób i podmiotów współpracujących w projekcie.
13. Obowiązki wynikające z ustawy o ochronie danych osobowych w zakresie podległych bezpośrednio Rektorowi pracowników i jednostek oraz osób i podmiotów współpracujących sprawuje osobiście ADO.
14. Pracownicy, współpracownicy i studenci, będący członkami organów kolegialnych i wyborczych Uczelni, a także członkami komisji, rad i innych zespołów powołanych przez organy Uczelni upoważniani są do przetwarzania danych osobowych w zakresie niezbędnym do pełnienia swych funkcji oraz zobowiązani do zachowania tajemnicy tych danych.
15. Nad obowiązkiem ochrony danych osobowych podczas obrad organów kolegialnych i wyborczych oraz komisji, rad i innych zespołów czuwa ich przewodniczący.
16. Dla organów oraz komisji, rad i innych zespołów, o których mowa w ust. 14, obowiązki wynikające z niniejszej Polityki i obowiązujących przepisów prawa realizuje jednostka obsługująca organ, komisję, radę lub inny zespół. W przypadku braku jednostki obsługującej, obowiązki wykonuje inna jednostka wskazana przez administratora danych.
17. Osoby prowadzące zajęcia dydaktyczne w Uczelni, są upoważniane do przetwarzania danych osobowych osób uczestniczących w zajęciach, w zakresie niezbędnym do pełnienia swych funkcji oraz zobowiązane do zachowania tajemnicy tych danych.
18. Przekazanie konkretnych zadań wskazanym wyżej osobom traktowane jest jak polecenie przetwarzania, w rozumieniu art. 29 RODO, wydane przez administratora.
19. LADO upoważnieni są do przetwarzania danych osobowych w podległych im obszarach oraz zobowiązani do zachowania tajemnicy tych danych.
20. LADO zobowiązani są do zapewnienia, w podległych im obszarach, przestrzegania przepisów prawa oraz zasad dotyczących przetwarzania danych osobowych oraz realizacji obowiązków z nich wynikających, w szczególności poprzez:
    a) identyfikowanie czynności przetwarzania danych osobowych realizowanych w podległym obszarze, określenie celów przetwarzania oraz podstawy prawnej przetwarzania danych osobowych wraz z kierującymi jednostek, a następnie powiadomienie o tym PDO ze wskazaniem informacji niezbędnych do zarejestrowania tych czynności w rejestrze czynności przetwarzania danych osobowych;
    b) określanie, wraz z kierującymi jednostkami, ryzyka naruszenia praw i wolności osób w procesie przetwarzania danych osobowych, oraz stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania prawa, w tym RODO, w podległych im obszarach;
    c) w przypadku konieczności powierzenia przetwarzania danych osobowych, wybór podmiotów przetwarzających, dających gwarancję przetwarzania zgodnego z RODO i zawieranie, zgodnych z wymaganiami art. 28 RODO, umów powierzenia przetwarzania;
    d) niezwłoczne, nie później niż w terminie 7 dni od daty zawarcia umowy, informowanie PDO o zawarciu, w podległym obszarze, umowy o powierzeniu przetwarzania danych osobowych, na podstawie której Uczelnia staje się podmiotem przetwarzającym - do informacji należy dołączyć kopię umowy lub jej skan;
    e) prowadzenie rejestru umów powierzenia przetwarzania danych osobowych, w formie pisemnej lub elektronicznej, zawierającego co najmniej datę zawarcia umowy i jej numer, nazwę podmiotu przetwarzającego, datę rozwiązania/wygaśnięcia umowy, stanowiącego załącznik nr 6 ;
    f) nadawanie i odwoływanie upoważnień do przetwarzania danych na podstawie składanych wniosków, których wzór stanowi załącznik nr 7, w formie pisemnej, osobom przetwarzającym dane osobowe w

zakresie wynikającym z zakresu obowiązków oraz prowadzenie ewidencji wydanych upoważnień, stanowiącego załącznik nr 4;

g) niezwłocznie przekazywanie jednego egzemplarza upoważnienia do Kadr w celu ich włączenia do akt osobowych pracownika, a kopii upoważnienia do PDO;
h) niezwłoczne informowanie PDO, nie później niż w terminie 7 dni od zdarzenia informacji o nadaniu, odwołaniu lub modyfikacji upoważnienia do przetwarzania danych osobowych;
i) przekazywanie ASI dokumentu nadającego uprawnienia w systemie informatycznym;
j) rozpatrywanie wniosków o udostępnianie danych;
k) uzyskiwanie zgód na przetwarzanie danych od osób (wg wzoru w załączniku nr 10), których dane Uczelnia pozyskuje, prowadzenie rejestru udzielonych zgód, stanowiącego załącznik nr 11, przechowywanie zgód, przechowywanie ewentualnych cofnięć zgód oraz podejmowanie stosownych działań w przypadku odwołania zgody lub upłynięcia terminu jej ważności,
l) zapoznanie osób, których dane pozyskuje Uczelnia, z informacjami o przetwarzaniu, gdy zbierane są nowe dane lub gdy zmienia się cel przetwarzania, a także dokumentowanie spełnienia tego obowiązku. Zakres przekazywanych informacji i przykładowy sposób poinformowania zawarte są w Załączniku Nr 9;
m) dopuszczanie do przetwarzania jedynie osób przeszkolonych w zakresie bezpieczeństwa danych osobowych i odpowiednio upoważnionych;
n) zapoznawanie osób zatrudnianych przy przetwarzaniu danych osobowych z obowiązującymi przepisami;
o) określanie zakresu indywidualnych obowiązków, uprawnień i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, w szczególności wprowadzenie ich do opisu stanowisk i zakresu obowiązków
p) stwarzanie właściwych warunków organizacyjno-technicznych, zapewniających ochronę danych osobowych w jednostce oraz ich zabezpieczenie przed dostępem osób nieupoważnionych, zmianą, utratą, uszkodzeniem lub zniszczeniem;
q) nadzorowanie fizycznego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolę przebywających w nich osób;
r) zapewnienie przestrzegania instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 1 do niniejszej Polityki;
s) zapewnienie przestrzegania instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, stanowiącej załącznik nr 11 do niniejszej Polityk, w szczególności przez podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.
t) zapewnienie przestrzegania obowiązujących ustaleń w zakresie udostępniania danych osobowych instytucjom i osobom spoza Uczelni;
u) analizowanie sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych oraz raportowanie do PDO;
v) zgłaszanie PDO zapotrzebowania na szkolenia w zakresie ochrony danych osobowych w jednostce organizacyjnej oraz zapewnienie ich przeprowadzenia;
w) bieżące aktualizowanie dokumentacji dotyczącej ochrony danych osobowych w zakresie jego obowiązującym;
x) zgłaszanie PDO projektów zarządzeń i innych dokumentów, w zakresie dotyczącym danych osobowych;
y) współdziałanie z PDO w zakresie przestrzegania zasad ochrony danych osobowych w Uczelni;
z) występowanie do ASI z wnioskiem o przydzielenie uprawnień w systemie informatycznym jeżeli dane przetwarzane są w formie elektronicznej, zawierającego opis uprawnień do przetwarzania danych, stanowiącego załącznik nr 7;
aa) zgłaszanie PDO planowanego utworzenia nowego zbioru (kategorii osób) lub modyfikacji istniejącego lub zmian w zakresie czynności dla istniejącego zbioru oraz przekazanie wszelkich informacji niezbędnych do rejestracji zbioru lub modyfikacji informacji na temat zbioru w rejestrze czynności przetwarzania.

21. LADO może wydawać, zgodnie z prawem, stosowne dokumenty normalizujące sposób przetwarzania danych osobowych w podległej jednostce organizacyjnej. Wydane dokumenty muszą być zaopiniowane przez PDO.
22. ASI w Uczelni, wyznaczony przez ADO, jest odpowiedzialny za:

bb) zapewnienie, aby do danych osobowych w systemie informatycznym miały dostęp wyłącznie osoby upoważnione w zakresie wykonywanych zadań,
cc) zarządzanie uprawnieniami do przetwarzania danych osobowych w systemie w imieniu ADO,
dd) nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których znajdują się serwery przetwarzające dane osobowe oraz kontroli przebywających w nich osób,
ee) nadzorowanie przestrzegania zasad określonych w Polityce i Instrukcji dotyczącej ochrony bezpieczeństwa danych osobowych,
ff) nadzorowanie wykonywania kopii awaryjnych, ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
gg) nadzorowanie przeglądów, konserwacji oraz uaktualnień systemów służących do przetwarzania danych osobowych oraz wszystkich innych czynności wykonywanych na bazach danych osobowych,
hh) nadzorowanie systemu komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji,
ii) nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe generowane przez system informatyczny,
jj) nadzorowanie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,
kk) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
ll) analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych, przygotowanie oraz przedstawienie ADO odpowiednich zmian do Instrukcji zarządzania systemem informatycznym,
mm) prowadzenie rejestru wydanych upoważnień przetwarzania danych,
nn) zlecenie modyfikacji uprawnień w systemach informatycznych w przypadku odebrania lub zmiany upoważnienia do przetwarzania danych osobowych,
oo) szkolenie osób dopuszczonych do przetwarzania danych osobowych z zasad pracy w systemie,
pp) nadzorowanie podpisania odpowiednich umów z firmami, którym powierzono przetwarzanie danych osobowych lub konserwacje urządzeń służących do przetwarzania danych oraz pracownikami tych firm z zachowaniem zasad określonych w rozdziale **Powierzenie przetwarzania danych osobowych** niniejszej Polityki, których przestrzeganie zapewnia PDO.

## 5. Pracownicy upoważnieni do przetwarzania danych osobowych

1. Osoby zatrudnione na Uczelni, bez względu na podstawę prawną zatrudnienia (na umowę o pracę, umowy cywilnoprawne), przetwarzające dane osobowe, niezależnie od celu i sposobu przetwarzania, są zobowiązane w szczególności do przestrzegania następujących zasad:
   a) mogą przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez ADO w upoważnieniu i tylko w celu wykonywania nałożonych na nie obowiązków; zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie; muszą zachować poufność danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania;
   b) przestrzeganie poufności danych osobowych obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji, albo po wygaśnięciu/rozwiązaniu umowy cywilnoprawnej łączącej te osoby z Uczelnią;
   c) są zobligowane do zapoznania się z przepisami prawa dotyczącymi ochrony danych osobowych oraz postanowieniami niniejszej Polityki bezpieczeństwa informacji w zakresie danych osobowych, w adekwatnym zakresie stosowania w odniesieniu do ochrony danych osobowych;
   d) muszą stosować określone przez ADO oraz PDO procedury oraz wytyczne mające na celu zgodne z prawem, w tym zawłaszcza adekwatne do wykonywanych przez nie zadań przetwarzanie danych;
   e) muszą korzystać z systemu informatycznego ADO oraz środowiska informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
   f) muszą zabezpieczyć przetwarzane dane osobowe przed dostępem osób nieupoważnionych;
   g) są zobowiązane zgłaszać LADO, a w przypadku jego nieobecności bezpośrednio PDO, wszelkie naruszenia dotyczące przetwarzania danych osobowych oraz podjąć konieczne działania dotyczące ograniczenia skutków naruszenia;

h) muszą stosować się do poleceń ADO oraz PDO w zakresie ochrony danych osobowych,
i) muszą stosować zasady postępowania osób upoważnionych do przetwarzania danych osobowych, określone w niniejszej Polityce.

2. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu.
3. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji, wygaśnięcie albo rozwiązanie umowy cywilnoprawnej albo wypowiedzenie upoważnienia przez ADO powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

## 6. Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych.
2. Upoważnienia nadają: Rektor, jako ADO oraz LADO.
3. Upoważnienie nadawane jest pracownikowi na pisemny wniosek bezpośredniego przełożonego upoważnianej osoby, którego wzór stanowi załącznik nr 7.
4. Upoważnienie nadawane jest współpracownikowi, w szczególności osobie wykonującej umowę cywilno-prawną, osobie odbywającej praktykę studencką, praktykę zawodową lub osobie w inny sposób związanej z Uczelnią, na pisemny wniosek kierownika jednostki zlecającej zadania związane z przetwarzaniem danych osobowych.
5. Upoważnienie jest nadawane pracownikom, współpracownikom i studentom, będących członkami organów kolegialnych i wyborczych Uczelni, a także członkami komisji, rad i innych zespołów powołanych przez organy Uczelni, na pisemny wniosek kierownika jednostki obsługującej organ, komisję, radę lub inny zespół.
6. Jeżeli osoba upoważniana (pracownik, osoba współpracująca) podlega nadającemu upoważnienie bezpośrednio, upoważnienie nadaje się bez wniosku.
7. Rektor, jako ADO oraz LADO, jako nadający upoważnienia mogą:
   a) wyrazić zgodę na nadanie uprawnień zgodnie z wnioskowanym zakresem lub na nadanie ograniczonych uprawnień zawierających się we wnioskowanym zakresie,
   b) nie wyrazić zgody na nadanie uprawnień.
8. Decyzja przekazywana jest osobie wnioskującej. W przypadku wydania decyzji o ograniczeniu uprawnień lub odmowy wydania upoważnienia, decyzja musi być sporządzona w formie pisemnej i zawierać uzasadnienie.
9. Od decyzji LADO wnioskujący może odwołać się do Rektora. Decyzja Rektora jest ostateczna.
10. Osoba wnioskująca przekazuje decyzję osobie uprawnianej.
11. Wszystkie nadane upoważnienia muszą być rejestrowane w rejestrach upoważnień (załącznik nr 4) prowadzonych odpowiednio przez:
    a) POD dla upoważnień nadanych przez Rektora
    b) LADO dla upoważnień przez siebie nadanych oraz ich poprzedników pełniących daną funkcję.
12. W przypadku jakiejkolwiek zmiany w prowadzonym przez LADO rejestrze (wpisanie upoważnienia, odebranie upoważnienia) przekazuje on kopię swojego zaktualizowanego rejestru PDO, który przechowuje wszystkie kopie rejestrów oraz rejestr upoważnień nadanych przez Rektora.
13. Nadanie upoważnienia do przetwarzania danych osobowych (w szczególności w systemie informatycznym) obejmuje:
    a) zapoznanie się osoby upoważnianej z niniejszą Polityką
    b) wydanie osobie upoważnianej upoważnienia do przetwarzania danych osobowych (załącznik nr 8),
    c) w przypadku przetwarzania danych osobowych w systemie informatycznym - nadanie osobie przez ASI identyfikatora oraz hasła, a także skonfigurowanie uprawnień w systemie.
14. W przypadku konieczności zmiany zakresu upoważnienia (inny lub kolejny zbiór osób, inny zakres przetwarzania danych osobowych, zmiana stanowiska pracy przez pracownika) należy przedłożyć LADO nowy wniosek o nadanie upoważnienia
15. W przypadku nadania osobie nowego upoważnienia dla danego zbioru osób, wygasa poprzednie upoważnienie.
16. Upoważnienie do przetwarzania danych osobowych sporządza się, w formie pisemnej, w dwóch egzemplarzach: jeden egzemplarz otrzymuje osoba upoważniona, drugi egzemplarz, w przypadku osób

upoważnionych będących pracownikami, przekazuje się do Kadr, a w przypadku osób upoważnionych, które nie są pracownikami pozostaje u LADO, który wydał upoważnienie. Kopia upoważnienia przekazywana jest do PDO. Wzory upoważnienia oraz odwołania upoważnienia zawarte są w załączniku Nr 8.

17. Odebranie upoważnienia do przetwarzania danych osobowych może mieć miejsce, gdy osoba upoważniona:
    a) przestała być pracownikiem lub współpracownikiem,
    b) utraciła potrzebę przetwarzania danych osobowych,
    c) spowodowała swoim celowym działaniem zagrożenie dla bezpieczeństwa przetwarzanych danych osobowych,
    d) przetwarza dane osobowe w sposób powodujący realne ryzyko utraty poufności, integralności lub dostępności tych danych.
18. Odebranie upoważnienia może nastąpić na wniosek: ADO lub LADO, ASI, bezpośredniego przełożonego pracownika, realizującego w imieniu Uczelni umowę osobą współpracującą, kierownika jednostki obsługującej organ, komisję, radę lub inny zespół.
19. Pisemny wniosek o odebranie upoważnienia (załącznik nr 8) jest przekazywany PDO i powinien zawierać: imię i nazwisko osoby, jej identyfikator do systemu informatycznego, zakres upoważnienia, które ma zostać odebrane, przyczyny złożenia wniosku.
20. W przypadku, gdy wnioskującym jest PDO, to przygotowuje on pisemną notatkę zawierająca informacje wymienione w pkt. poprzednim.
21. Jeżeli osoba, której upoważnienie zostało odebrane, posiadała dostęp do systemu informatycznego, to PDO przekazuje ASI polecenie unieważnienia hasła, zablokowania konta użytkownika, odebrania wszelkich uprawnień do systemu, które ASI powinien wykonać bez zbędnej zwłoki.
22. PDO informuje wnioskodawcę o odebraniu osobie upoważnienia do przetwarzania danych osobowych i o odebraniu (jeśli nastąpiło) uprawnień do systemu informatycznego.
23. Pracownicy nieposiadający w zakresie swoich obowiązków czynności związanych z przetwarzaniem danych osobowych (osoby sprzątające, portierzy, pracownicy techniczni, konserwatorzy, itp.), a których obowiązki wymuszają pracę - pod nieobecność osób upoważnionych do przetwarzania danych osobowych - w pomieszczeniach, w których dane osobowe są przetwarzane, muszą zostać zapoznane z zasadami dotyczącymi ochrony danych osobowych oraz uzyskać upoważnienie do przebywania w w/w pomieszczeniach wg wzoru w załączniku nr 13.
24. W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują wszystkie inne przepisy o tajemnicy służbowej, obiegu i zabezpieczeniu dokumentów służbowych.
25. Wszystkie osoby przetwarzające dane osobowe każdego rodzaju, niezależnie od systemu przetwarzania są zobowiązane w szczególności do:
    a) przetwarzania danych osobowych wyłącznie na polecenie administratora danych i w zakresie ustalonym indywidualnie w upoważnieniu i tylko w celu wykonywania nałożonych na nie obowiązków;
    b) zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po wygaśnięciu upoważnienia;
    c) posługiwania się niepowtarzalnym identyfikatorem dostępu do danych w systemie informatycznym;
    d) przestrzegania obowiązujących krajowych i wewnętrznych przepisów prawa w zakresie ochrony danych osobowych;
    e) korzystania z systemu informatycznego w sposób zgodny z niniejszą Polityką oraz zasadami pracy z systemem;
    f) zabezpieczania danych przed ich udostępnieniem osobom nieupoważnionym;
    g) natychmiastowego zgłaszania LADO, a w przypadku jego nieobecności bezpośrednio PDO zdarzeń naruszenia zabezpieczeń systemu informatycznego, zmian w sposobie działania programu lub urządzeń służących do przetwarzania danych.

## 7. Zasady zbierania danych osobowych

1. Każda osoba, której dane osobowe mają być przetwarzane musi zostać poinformowana przez ADO o:
    a) adresie siedziby ADO i jego pełnej nazwie,
    b) danych kontaktowych PDO,
    c) celach oraz podstawie prawnej przetwarzania danych,

d) prawnie uzasadnionych interesach realizowanych przez Uczelnię (jeśli dotyczy),
e) znanych lub potencjalnych odbiorcach danych,
f) o ewentualnym zamiarze przekazania danych osobowych do państwa trzeciego (poza obszar Unii Europejskiej) lub organizacji międzynarodowej,
g) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu,
h) prawie do żądania od Uczelni dostępu do jej danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
i) jeśli przetwarzanie odbywać się będzie na podstawie zgody osoby – prawie osoby do wycofania zgody,
j) prawie wniesienia skargi do organu nadzorczego (PUODO),
k) tym, 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,
l) ewentualnym profilowaniu,
m) źródle pochodzenia jej danych osobowych, jeżeli nie pozyskano ich od niej oraz tym, czy pochodzą one ze źródeł publicznie dostępnych.

2. Informacji należy udzielić przed uzyskaniem od osoby jej danych za pomocą klauzuli informacyjnej zawartej w załączniku nr 9.
3. Każda osoba musi zostać poinformowana o zmianie celu przetwarzania na inny niż cel, w którym dane zostały zebrane.
4. W przypadku kandydatów na pracowników oświadczenie o poinformowaniu osoby przez Uczelnię o okolicznościach wskazanych w ust. 1. wraz z podpisem kandydata na pracownika przyjmują i przechowują Kadry razem z dokumentacją kandydata.
5. W przypadku osób zatrudnianych na podstawie umowy o pracę (nowych pracowników) informacja określona w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uczelnię zawarte muszą być na druku kwestionariusza osobowego.
6. W przypadku kandydatów na studia informacja określona w ust. 1. umieszczona musi być na pierwszej stronie internetowego systemu rekrutacji. By przejść do kolejnych etapów rejestracji, kandydat musi potwierdzić, że został o w/w okolicznościach poinformowany. Oświadczenie osoby o jej poinformowaniu przez Uczelnię przechowywane jest w formie elektronicznej.
7. W przypadku osób zatrudnianych na podstawie umowy cywilno-prawnej informacja określona w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uczelnię zawarte muszą być na druku umowy.
8. W przypadku pozostałych kategorii osób obowiązek informacyjny musi być zrealizowany z wykorzystaniem klauzuli informacyjnej stanowiącej załącznik nr 9 oraz oświadczenie osoby o jej poinformowaniu przez Uczelnię. Druk zawierający stosowna klauzulę przekazuje osobie do podpisu i później przechowuje jednostka przyjmująca do przetwarzania dane osoby.
9. Bezwzględnie zabronione jest kopiowanie (skanowanie, kserowanie itp.) dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, jak również żądanie od osoby czasowego pozostawienia takiego dokumentu.

## 8. Rejestrowanie przetwarzania danych osobowych

1. Uczelnia jako administrator prowadzi rejestr czynności przetwarzania, zgodnie ze strukturą i zawartością pól informacyjnych określonymi w załączniku nr 2 i zawierający następujące informacje, wymagane przez RODO:
   a) nazwa oraz dane kontaktowe Uczelni oraz wszelkich współadministratorów, w rozumieniu art. 26 RODO, a także inspektora ochrony danych;
   b) cele przetwarzania;
   c) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

2. Uczelnia jako podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu innego administratora, zgodnie ze strukturą i zawartością pól informacyjnych określonymi w załączniku nr 3 i zawierający następujące informacje, wymagane przez RODO:
   a) nazwa oraz dane kontaktowe Uczelni lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa Uczelnia, a gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
   b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
   c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
   d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
3. Prowadzenie rejestrów określonych w ust. 1 i 2 tworzonych na podstawie informacji otrzymanych od kierujących jednostkami, jest zadaniem PDO.

## 9. Przetwarzanie danych biometrycznych

1. Wykorzystanie danych biometrycznych w postaci wizerunku osoby na stronach internetowych ADO oraz materiałach reklamowych rozpowszechnianych przez ADO wymaga uzyskania od tej osoby pisemnej zgody na korzystanie z wizerunku, jego publikację oraz przetwarzanie danych biometrycznych.
2. Obowiązek pozyskania zgody na publikację wizerunku nie dotyczy osób powszechnie znanych w związku z pełnieniem przez nich funkcji publicznych, w szczególności politycznych, społecznych, zawodowych.
3. Obowiązek pozyskania zgody na publikację wizerunku nie dotyczy osoby stanowiącej jedynie szczegół całości takiej, jak zgromadzenie, krajobraz, publiczna impreza.
4. Przetwarzanie danych osobowych dla celów wydarzeń organizowanych przez Uczelnię może się odbywać wyłącznie na podstawie stosownych upoważnień do przetwarzania danych osobowych.
5. Za obowiązek zamieszczenia obowiązkowych klauzul informacyjnych w materiałach promujących wydarzenie odpowiada kierownik jednostki organizującej wydarzenie w porozumieniu z LADO. Wzór klauzuli informacyjnej ADO stanowi Załącznik nr 9 do niniejszej Polityki bezpieczeństwa informacji w zakresie danych osobowych.
6. Kierownik jednostki organizującej wydarzenie jest zobowiązany pozyskać oświadczenia w przedmiocie udzielenia zgody na przetwarzanie danych osobowych od osób, których dane osobowe będą przetwarzane dla celów organizacji wydarzenia.
7. Wzór oświadczenia w przedmiocie udzielenia zgody na przetwarzanie danych osobowych zostanie opracowany każdorazowo, przez LADO i zatwierdzony przez PDO, dla danego wydarzenia, z uwzględnieniem specyfiki wydarzenia, z rozdzieleniem czynności i celów przetwarzania, z wykorzystaniem wzorów w załączniku nr 10.

## 10. Udostępnianie danych osobowych

1. Udostępnianie danych osobowych instytucjom i osobom spoza Uczelni może odbywać się wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, wyłącznie w przypadkach, gdy udostępnienie danych nie narusza prawa i wolności osób, których udostępniane dane dotyczą.
2. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis szczególny stanowi inaczej.
3. Wniosek o udostępnienie danych powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz określać: rodzaj i zakres danych, formę ich przekazania lub udostępnienia, cel, w jakim dane mają zostać udostępnione.
4. W przypadku wniosku o udostępnienie kierowanego przez instytucję wniosek powinien zawierać również wskazanie osoby po stronie wnioskodawcy upoważnionej do pobrania danych lub zapoznania się z nimi.
5. Dane osobowe udostępniane są przez PDO za pośrednictwem LADO w podległych im obszarach.

6. Udostępnianie danych osobowych organom ścigania i innych służbom publicznym na podstawie upoważnień wynikających z powszechnie obowiązujących przepisów prawa może nastąpić tylko na pisemny wniosek skierowany do ADO i za jego zgodą. Wniosek ten powinien zawierać:
   a) oznaczenie wnioskodawcy;
   b) wskazanie przepisów uprawniających do dostępu do informacji;
   c) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia;
   d) wskazanie osoby po stronie wnioskodawcy upoważnionej do pobrania informacji lub zapoznania się z ich treścią.
7. PDO prowadzi ewidencję danych osobowych udostępnianych odbiorcom danych i organom publicznym innym niż odbiorcy danych.
8. Udostępnianie danych osobowych odbiorcom danych i organom publicznym innym niż odbiorcy danych może odbywać się wyłącznie za pośrednictwem PDO.
9. PDO prowadzi rejestr udostępnień wg załącznika nr 14, w którym odnotowywane są informacje o odbiorcach i udostępnieniach

## 11. Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu może się odbywać wyłącznie na mocy zawartej w formie pisemnej umowy powierzenia, która musi określać w szczególności: zakres i cel przetwarzania danych, specyfikację zbioru danych osobowych podlegającego powierzeniu, obowiązki ADO oraz obowiązki i odpowiedzialność podmiotu, któremu powierzono przetwarzanie danych.
2. Umowę przygotowuje jednostka organizacyjna powierzająca przetwarzanie danych osobowych w porozumieniu z właściwym LADO.
3. Wszystkie umowy dotyczące powierzenia danych osobowych, powinny zostać przed podpisaniem zaopiniowane przez PDO.
4. W uzasadnionych przypadkach PDO może nie wyrazić zgody na powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu.
5. Wszystkie umowy powierzenia powinny być wpisane do rejestru umów powierzenia stanowiącego załącznik nr 6 do niniejszej Polityki (co najmniej datę zawarcia umowy i jej numer, nazwę podmiotu przetwarzającego, datę rozwiązania/wygaśnięcia umowy;
6. Podmiot, któremu powierzone zostało przetwarzanie danych obowiązany jest przed rozpoczęciem ich przetwarzania podjąć środki mające na celu zabezpieczenie zbioru danych, spełniające wymagania określone w ustawie.

## 12. Środki organizacyjne i techniczne ochrony danych

1. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.
2. W celu właściwej ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.
3. Zastosowane środki ochrony powinny wynikać z okresowego przeglądu i analizy zagrożeń oraz szacowania ryzyka dla procesów przetwarzania danych osobowych.
4. Za przeprowadzenie czynności określonych w pkt.3 odpowiadają: LADO w podległych im obszarach oraz PDO dla całej Uczelni.

## 13. Obszar przetwarzania danych osobowych

1. Obszary przetwarzania danych osobowych są określane przez właściwego LADO w porozumieniu z PDO i powinny obejmować:
   a) pomieszczenia lub ich części, w których wykonuje się operacje na danych osobowych tzn. wpisuje, modyfikuje, kopiuje, szczególnie wykonywane w systemie informatycznym;
   b) pomieszczenia lub ich części, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe, m.in. szafy z dokumentacją papierową bądź komputerowymi nośnikami informacji, z

kopiami zapasowymi danych, komputery stanowiskowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe).

c) pomieszczenia lub ich części, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, niesprawne komputery i inne urządzenia z nośnikami zawierającymi dane osobowe)

d) pomieszczenia lub ich części np. sejfy, jeśli przechowuje się w nich elektroniczne nośniki informacji zawierające kopie zapasowe danych przetwarzanych w systemie informatycznym czy też inne nośniki danych, np. dokumentów źródłowych.

2. LADO w porozumieniu z PDO wnioskuje do Kanclerza Uczelni o właściwe wyposażenie obszaru przetwarzania, gwarantujące adekwatną ochronę przetwarzanych danych osobowych.
3. Do obszaru przetwarzania danych osobowych właściwy LADO powinien zaliczyć również miejsce w sejfie bankowym, archiwum itp., jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym czy też do składowania innych nośników danych, np. dokumentów źródłowych.
4. LADO opracowuje wykaz pomieszczeń i powierzchni stanowiących podległy mu wg wzoru stanowiącego załącznik nr 12.
5. LADO przekazuje kopię wykazu PDO po określeniu obszaru i każdorazowo po jego zmianie.
6. Szczegółowe zasady kontroli dostępu do poszczególnych pomieszczeń w obszarach przetwarzania określane są przez LADO.
7. W obszarze przetwarzania mają prawo przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę przetwarzania i ochrony tych danych.
8. Ewidencje osób upoważnionych do dostępu do pomieszczeń w obszarze przetwarzania tworzy i aktualizuje LADO wg załącznika nr 4.
9. Osoby nieposiadające upoważnienia do przetwarzania danych osobowych, w szczególności: serwisujące urządzenia, sprzątające, konserwujące, remontujące, chroniące budynek, mogą przebywać w obszarze przetwarzania wyłącznie w obecności upoważnionego pracownika Uczelni lub na podstawie dokumentu wydanego przez LADO zezwalającego i określającego warunki przebywania w tym obszarze.
10. Zezwolenie na przebywanie w obszarze przetwarzania na określonych warunkach może wynikać z umowy zawartej z podmiotem realizującym usługi.
11. Jeżeli obszar przetwarzania zajmuje jedynie część pomieszczenia, to należy go wyraźnie oddzielić od części ogólnodostępnej, np. za pomocą barierek, lad lub odpowiednie ustawienie mebli biurowych, aby skutecznie uniemożliwić niekontrolowany dostęp osób nieupoważnionych.
12. W obszarze przetwarzania należy bezwzględnie przestrzegać:
    a) zasady czystego biurka, czyli niepozostawiania na biurku jakiejkolwiek dokumentacji albo nośników danych zawierających dane osobowe;
    b) obowiązku przechowywania dokumentów i nośników zawierających dane osobowe w meblach zamykanych na klucz;
    c) obowiązku wyłączania komputera lub wygaszania ekranu monitora komputera podczas czasowej nieobecności albo wizyty osoby nieposiadającej upoważnienia ADO do przetwarzania danych osobowych.
13. W razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych należy umieścić zbiory występujące w formach tradycyjnych oraz na nośnikach danych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobom niepowołanym (np. wylogowanie się, włączanie blokady komputera, uruchamianie wygaszacza ekranu odblokowywanego hasłem, itp.).
14. Wszystkie pomieszczenia, w których przetwarza się dane osobowe muszą być zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy.
15. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia i/lub umiejscowionych w nim zbiorów danych jest niedopuszczalne, i traktowane jest jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
16. Zasady bezpiecznego przechowywania i udostępniania kluczy do pomieszczeń wchodzących w skład obszaru przetwarzania wraz z określeniem odpowiedzialności poszczególnych osób opracowuje i wdraża LADO.
17. Czynności wydania i zwrotu kluczy do pomieszczeń są ewidencjonowane, w ten sposób, że w ewidencji poboru i zwrotu kluczy odnotowywane jest nazwisko osoby pobierającej albo zdającej klucz, godzina

pobrania albo zdania oraz numer lub inne oznaczenie pomieszczenia, do którego klucz jest pobierany albo zwracany.

18. Niedozwolone jest wykonywanie oraz używanie osobistych kopii kluczy do pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych.
19. Zakazane jest pozostawienie niezabezpieczonego pomieszczenia należącego do obszaru przetwarzania bez nadzoru.
20. W przypadku opuszczenia stanowiska pracy znajdującego się w obszarze przetwarzania należy zabezpieczyć dane osobowe przed nieupoważnionym dostępem.
21. W toku wykonywania obowiązków służbowych, w ramach których przetwarzane są dane osobowe należy stosować zasadę wykorzystywania danych osobowych wyłącznie w zakresie koniecznym dla celów przetwarzania.
22. W toku wykonywania obowiązków służbowych należy, uniemożliwić osobom nieupoważnionym dostęp do danych osobowych oraz ich przetwarzanie.

## 14. Zagrożenia i ryzyko przetwarzania danych osobowych

1. Zagrożenia przetwarzania danych osobowych mogą powodować utratę:
   a) poufności, czyli udostępnienie danych osobie nieupoważnionej;
   b) integralności, czyli dopuszczenie do nieupoważnionej zmiany danych lub ich zniszczenia;
   c) rozliczalności, czyli braku możliwości przypisania ADO w sposób jednoznaczny działań zgodnych z zasadami przetwarzania danych określonymi przez RODO (art.5 ust.2).
2. W zależności od lokalizacji źródła zagrożenia dzieli się je na dwie grupy:
   a) wewnętrzne (np. działania pracownika, działania ASI, awaria systemu, awaria sprzętu, błędy oprogramowania, awaria zasilania), w wyniku których może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu informatycznego, może nastąpić naruszenie poufności danych;
   b) zewnętrzne (np. klęski żywiołowe, pożary, zalania, przerwy w zasilaniu energii), w wyniku których może dojść do utraty integralności danych lub ich zniszczenia (zarówno danych przetwarzanych w formie tradycyjnej papierowej, jak i elektronicznej) lub uszkodzenia infrastruktury technicznej systemu informatycznego, przy czym ciągłość pracy systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych;
3. W zależności od przyczyny zagrożenia dzieli się na:
   a) działanie przypadkowe człowieka (np. niezamierzone skasowanie pliku czy uszkodzenie urządzenia)
   b) działanie umyślne człowieka (świadome i celowe naruszenia poufności danych przez np. kradzież sprzętu zawierającego dane osobowe lub dokumentów zawierających dane, nieuprawniony dostęp do systemu wewnątrz sieci uczelnianej i modyfikacja danych lub nieuprawnione przekazanie danych, włamanie do systemu z zewnątrz sieci uczelnianej)
   c) naturalne (np. pożary, zalania)
4. Opisane w pkt 1-3 zagrożenia przetwarzania danych osobowych mogą powodować naruszenia tych danych.
5. W przypadku wystąpienia naruszeń należy postępować zgodnie z Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych stanowiącą załącznik nr 11 do niniejszej Polityki.
6. Kierownicy jednostek organizacyjnych, w których przetwarzane są dane osobowe zobowiązani są do stałego monitorowania zagrożeń związanych z przetwarzaniem w ramach ich jednostki danych osobowych, a następnie, w porozumieniu z LADO, do analizy ryzyka w tym obszarze.
7. Analiza ryzyka powinna dotyczyć zmian w stosunku do wstępnej analizy zawartej w załączniku nr 16 i obejmować wzrost ryzyka przetwarzania danych związany w szczególności:
   a) ze zmianami w przepisach regulujących zasady ochrony danych osobowych,
   b) ze stwierdzenia naruszeń ochrony danych,
   c) z wprowadzenia modyfikacji procesu przetwarzania danych osobowych, w określonym istniejącym zbiorze,
   d) z planowaniem tworzenia nowego zbioru danych osobowych i jego przetwarzania,
   e) z planowaniem powierzenia przetwarzania danych podmiotowi zewnętrznemu,
   f) z planowaniem przyjęcia powierzenia przetwarzania danych od podmiotu zewnętrznego.
8. W przypadku stwierdzenia wzrostu ryzyka, LADO, w uzgodnieniu z PDO ustala, a następnie wdraża rozwiązania minimalizujące ryzyko.

## 15. Środki organizacyjne i techniczne zapewniające ochronę danych osobowych w zakresie poufności, integralności i rozliczalności.

1. Dane osobowe mogą przetwarzać wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają, oraz sposoby ich zabezpieczenia.
2. Fakt modyfikacji zbioru danych: struktury, lokalizacji, a także utworzenia zbioru ASI ma obowiązek zgłosić PDO.
3. Dane osobowe w postaci papierowej oraz w postaci elektronicznej (m.in. płyty, pendrive'y) są przechowywane po zakończeniu pracy w zamykanych na klucz meblach biurowych (szafy, komody, szuflady, itp.), a tam, gdzie jest to możliwe – w szafach metalowych.
4. Sposób zabezpieczenia kluczy do mebli biurowych lub szaf metalowych, służących do przechowywania danych osobowych przed dostępem osób nieupoważnionych określa LADO.
5. W przypadku braku możliwości umieszczenia wszystkich dokumentów i nośników zawierających dane osobowe w zamykanych meblach, należy zrezygnować w tym dniu z wykonania usługi sprzątania.
6. Dane osobowe w wersji papierowej, a także wydruki i kopie, należy niszczyć w niszczarkach lub przekazywać do zniszczenia wynajętej do tego celu firmie. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.
7. Serwery zlokalizowane są w odrębnych, klimatyzowanych pomieszczeniach - serwerowniach, których okna odpowiednio zabezpieczone przed dostępem z zewnątrz, a drzwi zamykane na zamek.
8. Dostęp do serwerowni mają jedynie upoważnieni pracownicy obsługujący serwery. Inne osoby upoważnione do przetwarzania danych osobowych mają dostęp wyłącznie w ich obecności.
9. Wszystkie serwery są zasilane za pośrednictwem zasilaczy awaryjnych.
10. Bieżąca konserwacja serwerów oraz komputerów osobistych prowadzona jest tylko przez upoważnionych pracowników.
11. W przypadku konieczności naprawy lub konserwacji sprzętu w serwerowni przez pracowników zewnętrznej firmy należy zawrzeć z nią umowę o powierzenie przetwarzania danych osobowych ze szczególnym uwzględnieniem kar umownych za naruszenie bezpieczeństwa danych.
12. Konserwowanie i naprawa serwerów oraz komputerów osobistych poza siedzibą Uczelni dopuszczalne jest jedynie po trwałym usunięciu danych osobowych.
13. Zużyty sprzęt może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.
14. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez ASI.
15. Komputery, monitory, drukarki oraz inne urządzenia służące do przetwarzania, a zwłaszcza kopiowania danych, powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym podgląd informacji oraz bezpośredni i niekontrolowany dostęp.
16. Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami zabezpieczonymi hasłem.
17. Stanowisko pracy może być opuszczone dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób.
18. Dane osobowe na pamięciach przenośnych powinny być kasowane natychmiast po ich wykorzystaniu, a płyty skutecznie niszczone.
19. Osoby upoważnione do przetwarzania danych osobowych nie mogą samodzielnie ingerować w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych).
20. Osoby upoważnione do przetwarzania danych osobowych są obowiązane do przestrzegania swoich uprawnień w systemie, w szczególności używania tylko własnego identyfikatora i hasła dostępu.
21. Hasło wymagane do uwierzytelnienia się w systemie nie może być zapisywane na papierze lub innym nośniku.
22. Przesyłanie danych osobowych pocztą elektroniczną jest dopuszczalne wyłącznie w postaci zaszyfrowanej.
23. Zabronione jest wynoszenie poza obiekty Uczelni danych osobowych w jakiejkolwiek formie, zarówno papierowej, jak i elektronicznej, nawet zaszyfrowanej, za wyjątkiem ich przekazywania pomiędzy jednostkami organizacyjnymi znajdującymi się w różnych lokalizacjach.

24. Komputery oraz inne urządzenia informatyczne, przy pomocy których przetwarzane są dane osobowe, powinny posiadać wydzielony obwód zasilania, dedykowany dla sprzętu informatycznego.
25. Do gniazdek zasilających sprzęt komputerowy, również za pośrednictwem listew zasilających, nie wolno podłączać innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).
26. W przypadku planowanych wyłączeń zasilania, administrujący budynkiem musi bezwzględnie poinformować o tym odpowiednio wcześniej wszystkie jednostki organizacyjne, w których dane osobowe przetwarzane są z wykorzystaniem systemów informatycznych, tak by przed wyłączeniem zasilania można było w bezpieczny sposób zakończyć przetwarzanie danych w systemie.
27. Zabronione jest przetwarzanie danych osobowych w zewnętrznych systemach informatycznych (np. w „chmurze") bez zgody ADO.
28. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczane poprzez tworzenie kopii zapasowych umożliwiających odtworzenie danych w przypadku awarii.
29. Za wykonywanie kopii odpowiada ASI lub inny pracownik upoważniony przez LADO na wniosek ASI.
30. Kopie zapasowe tworzone na zewnętrznych nośnikach informatycznych (na taśmach, pendrive'ach, płytach CD, DVD itp.) muszą być przechowywane w szafach, szufladach lub pomieszczeniach zamykanych na klucz, do których dostęp mają jedynie osoby odpowiedzialne za wykonywanie i zabezpieczanie tych kopii.
31. Kopie należy przechowywać w innym pomieszczeniu (a w miarę możliwości innym budynku), niż to, w którym znajduje się (na przykład na serwerze) oryginalny, wykorzystywany w bieżącej pracy zbiór danych.
32. W komputerach, w których nie ma potrzeby wykorzystywania zewnętrznych nośników danych (pendrive'ów, płyt CD/DVD, dysków zewnętrznych itp.) należy w miarę możliwości zablokować możliwość zapisu na płytach CD/DVD oraz porty USB, by ograniczyć możliwość kopiowania danych osobowych na takie nośniki.
33. Robocze, błędne lub nieaktualne wydruki oraz kopie danych tworzone na nośnikach informatycznych należy usuwać (niszczyć) natychmiast po ustaniu ich przydatności.
34. Niedopuszczalne jest pozostawianie po zakończeniu pracy w danym dniu dokumentów, wydruków zawierających dane osobowe w drukarkach, kserokopiarkach, skanerach i tym podobnych urządzeniach.
35. Niepotrzebne już dokumenty w formie papierowej zawierające dane osobowe muszą zostać zniszczone w sposób uniemożliwiający ich odczytanie, to jest przy pomocy niszczarki.
36. Procedurę zarządzania uprawnieniami do systemów informatycznych oraz sposoby zabezpieczenia danych osobowych przed utratą i uszkodzeniem reguluje „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", stanowiąca załącznik nr 1 do niniejszej Polityki.
37. W przypadku naprawy, przekazania, likwidacji nośnika (papier, dysk twardy, płyta kompaktowa, dyskietka, taśma magnetyczna), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe.
38. W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy zachować szczególną ostrożność podczas używania komputera poza obszarem przetwarzania danych wyszczególnionym w niniejszej Polityce. W szczególności należy stosować mechanizmy szyfrowania plików lub baz danych rekomendowane przez ASI. Po ustaniu konieczności przetwarzania danych na komputerze przenośnym, należy je trwale usunąć z nośnika danych.
39. Operacje za pośrednictwem rachunku bankowego ADO może wykonywać wyłącznie pracownik, upoważniony przez Rektora, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.
40. Na stronie www Uczelni lub w jakiejkolwiek innej formie dozwolone jest publikowanie następujących danych osobowych pracowników: imię, nazwisko, stanowisko, służbowy numer telefonu, służbowy adres e-mail.
41. Publikowanie na stronach www Uczelni lub w jakiejkolwiek innej formie innych danych pracowników (w tym prywatnych numerów telefonów, prywatnych adresów e-mail, adresów prywatnych stron WWW, wizerunku pracownika itp.) jest zabronione, chyba, że pracownik wyrazi na to zgodę w formie pisemnej.
42. Zgoda, o której mowa w ust. 42 przechowywana jest przez właściwego LADO oraz POD.
43. Zabronione jest przekazywanie danych osobowych osobom nieuprawnionym telefonicznie, elektronicznie lub w jakiejkolwiek innej formie.
44. Dokumenty zawierające dane osobowe, przenoszone lub przewożone pomiędzy jednostkami Uczelni znajdującymi się w różnych lokalizacjach muszą być zamknięte w zaklejonej kopercie i opieczętowane w taki sposób, aby były widoczne próby ewentualnego otwarcia przez osoby nieupoważnione.

45. Przekazywanie w ramach jednostki organizacyjnej lub pomiędzy jednostkami nośników informatycznych lub dokumentów zawierających dane osobowe, może odbywać się tylko pomiędzy osobami posiadającymi upoważnienia do przetwarzania danych osobowych określonych zbiorów osób.

## 16. Monitorowanie przestrzegania Polityki oraz przepisów prawa i aktów wewnętrznych dotyczących ochrony danych osobowych

1. W ramach monitorowania POD ma prawo dokonania kontroli stanu przestrzegania Polityki oraz przepisów prawa i aktów wewnętrznych dotyczących ochrony danych osobowych
2. Czynności kontrolne w zakresie systemów informatycznych wykonuje ASI w porozumieniu z POD.
3. Po zakończeniu kontroli sporządzany jest protokół zawierający opis zakresu kontroli i opis przeprowadzonych czynności, którego wzór stanowi załącznik nr .
4. Inspektor Ochrony Danych przedstawia w sprawozdaniu stwierdzone w wyniku sprawdzenia uchybienia, wnioski i zalecenia mające służyć usunięciu uchybień oraz termin realizacji zaleceń.

## 17. Przeglądy i aktualizacje Polityki

1. POD dokonuje przynajmniej raz do roku przeglądu Polityka bezpieczeństwa pod kątem aktualności.
2. Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:
   a) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji Polityki,
   b) innych znaczących zmian dotyczących danych osobowych w funkcjonowaniu Uczelni.
3. Aktualizacji Polityki dokonuje Pełnomocnik Danych, a zatwierdza ją Administrator Danych.

## 18. Postanowienia końcowe

1. Niniejsza wersja Polityki bezpieczeństwa przetwarzania danych osobowych wchodzi w życie z dniem 15.10.2018 r.

## Załączniki

1. Instrukcja zarządzania systemem informatycznym.
2. Rejestr czynności przetwarzania danych osobowych.
3. Rejestr kategorii czynności przetwarzania danych osobowych w imieniu administratora.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
5. Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych.
6. Rejestr umów powierzenia przetwarzania danych osobowych.
7. Wniosek o upoważnienie do przetwarzania danych osobowych.
8. Upoważnienie do przetwarzania danych osobowych.
9. Klauzula informacyjna.
10. Zgody na przetwarzanie danych osobowych
11. Rejestr udzielonych zgód na przetwarzanie danych osobowych.
12. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.
13. Obszar przetwarzania danych osobowych
14. Upoważnienie do przebywania w obszarze przetwarzania danych osobowych.
15. Ewidencja udostępniania danych
16. Oświadczenie o odbyciu szkolenia.