Załącznik
do Zarządzenia Nr 36/2018
Rektora UWM w Olsztynie
z dnia 28 maja 2018 roku

Polityka Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie

UNIWERSYTET
WARMIŃSKO-MAZURSKI
W OLSZTYNIE

Olsztyn, 2018

Spis treści

Wstęp

Misją Uniwersytetu Warmińsko-Mazurskiego w Olsztynie jest:

„Pomnażanie kapitału intelektualnego służącego zrównoważonemu rozwojowi regionu i kraju poprzez tworzenie przyjaznych warunków do kreowania i zdobywania wiedzy".

Gwarancją realizacji Misji Uniwersytetu jest sprawna i skuteczna ochrona informacji i danych osobowych poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych. Władze Uniwersytetu Warmińsko-Mazurskiego w Olsztynie świadome wagi problemów związanych z bezpieczeństwem informacji i ochroną prawa do prywatności, w tym w szczególności praw osób fizycznych powierzających Uniwersytetowi swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklarują:

- zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
- zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Uniwersytecie Warmińsko – Mazurskim w Olsztynie w zakresie problematyki bezpieczeństwa informacji,
- zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,
- zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

Ponadto, władze Uniwersytetu Warmińsko – Mazurskiego w Olsztynie świadome zagrożeń związanych z przetwarzaniem przez Uczelnię danych osobowych na dużą skalę oraz posiadania w swych zbiorach innych informacji podlegających ochronie – w tym w szczególności, zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych informacji w systemach informatycznych oraz sieciach telekomunikacyjnych deklarują, że zamierzają doskonalić i rozwijać nowoczesne metody przetwarzania danych w oparciu o najwyższej jakości standardy bezpieczeństwa.

§ 1

Cel i zakres unormowań

1. Polityka Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie określa strukturę organizacyjną zapewniającą optymalny podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem adekwatnego i proporcjonalnego stopnia bezpieczeństwa informacji i danych osobowych administrowanych przez Uniwersytet, przetwarzanych zarówno metodami tradycyjnymi, jak i z wykorzystaniem systemów informatycznych.
2. Niniejszy dokument wyznacza podmioty odpowiedzialne za przetwarzanie danych osobowych i informacji oraz zobowiązuje je do zapewnienia możliwie najwyższego poziomu bezpieczeństwa.
3. Integralną częścią Polityki są następujące załączniki:
   1) wzór klauzuli zgody na przetwarzanie danych osobowych,
   2) wzór klauzuli informacyjnej Administratora Danych,
   3) rejestr czynności przetwarzania danych,
   4) upoważnienie do przetwarzania danych,
   5) oświadczenie o zachowaniu w tajemnicy danych osobowych i informacji oraz sposobów ich zabezpieczenia,
   6) ewidencja osób upoważnionych do przetwarzania danych,
   7) ewidencja użytkowników z uprawnieniami do systemów informatycznych,
   8) wzór umowy na powierzenie przetwarzania danych osobowych,
   9) rejestr naruszeń ochrony danych osobowych i bezpieczeństwa informacji.
4. Opracowane w dokumencie zasady, prawa oraz procedury opierają się na przepisach powszechnie obowiązujących, przy czym pierwszeństwo w stosowaniu mają zawsze te drugie. Polityka ma na celu zgromadzenie i opisanie w sposób przystępny podstawowych zasad postępowania z danymi osobowymi i informacjami w celu zapewnienia odpowiedniego poziomu ich ochrony.
5. Polityka została opracowana w celu spełnienia wymogów wynikających z przepisów prawa, w szczególności:
   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 (Dz. Urz. UE L 119);
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   3) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113).

6. Zakres obowiązywania Polityki obejmuje:
   1) wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz tradycyjne dokumenty (papierowe), w których przetwarzane są lub będą dane osobowe i informacje;
   2) informacje będące własnością Uniwersytetu, partnerów lub osób korzystających z usług Uniwersytetu, o ile zostały przekazane na podstawie umów;
   3) wszystkie typy nośników (np. papierowych, magnetycznych, optycznych, itp.), na których są lub będą znajdować się dane osobowe lub informacje;
   4) wszystkie lokalizacje – pomieszczenia i części pomieszczeń, w których są lub będą przetwarzane dane osobowe lub informacje;
   5) wszystkich pracowników w rozumieniu przepisów Kodeksu pracy oraz inne osoby mające dostęp do danych osobowych lub informacji.
7. Ponadto, celem opracowania i wdrożenia Polityki jest osiągnięcie poziomu organizacyjnego i technicznego, który:
   1) będzie gwarantem pełnej ochrony osób, których dane dotyczą oraz ciągłości procesu ich przetwarzania;
   2) zapewni zachowanie poufności informacji chronionych oraz legalności, przejrzystości, rzetelności, celowości, adekwatności, prawidłowości, czasowości, integralności i poufności przetwarzania danych osobowych osób fizycznych;
   3) zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach i formach jej przetwarzania;
   4) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji i danych osobowych, wynikających z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Uniwersytetu;
   5) zapewni gotowość do podjęcia działań w sytuacjach zagrożenia dla bezpieczeństwa Uniwersytetu, jego interesów oraz posiadanych i powierzonych mu informacji i danych osobowych.
8. Przegląd oraz aktualizacja Polityki i procedur postępowania dokonywane są przez Inspektora Ochrony Danych Uniwersytetu oraz pracowników zaangażowanych przez Administratora Danych w prace na rzecz skutecznego stosowania przepisów w zakresie ochrony danych osobowych.
9. Organizacyjne, techniczne oraz informatyczne środki ochrony informacji i danych osobowych przewidziane w Polityce formułowane są w oparciu o występujące ryzyko związane z zagrożeniami, takimi jak:
   1) błędy i nieprawidłowości w postępowaniu własnych pracowników,
   2) naturalne katastrofy,
   3) działalność przestępcza,

4) infekcje systemów informatycznych, które mogą wykradać zasoby komputera,
5) korzystanie z witryn internetowych na których zainstalowane są skrypty pozwalające wykradać zasoby komputera,
6) przerwy i zakłócenia w działaniu systemu,
7) inne zagrożenia mogące wystąpić w związku z socjotechnicznymi metodami kradzieży informacji oraz dynamicznie rozwijającymi się technikami i metodami przetwarzania danych.

§ 2

Skróty i definicje

1. ***Uniwersytet*** – oznacza Uniwersytet Warmińsko-Mazurski w Olsztynie.
2. ***Polityka*** **–** oznacza Politykę Bezpieczeństwa Informacji, określoną w niniejszym dokumencie.
3. ***Administrator Danych*** **–** Uniwersytet Warmińsko-Mazurski w Olsztynie decydujący o celach i środkach przetwarzania danych osobowych.
4. ***Inspektor lub IOD*** **–** Inspektor Ochrony Danych.
5. ***Administrator Systemu Informatycznego*** **–** pracownik Uniwersytetu nadzorujący pracę systemu informatycznego oraz wykonujący w nim czynności wymagających specjalnych uprawnień.
6. ***RODO*** **–** 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.
7. ***Pracownik*** **–** osoba zatrudniona w Uniwersytecie w oparciu o umowę o pracę, akt mianowania lub realizująca zlecone czynności na podstawie umowy cywilnoprawnej.
8. ***Użytkownik*** **–** osoba posiadająca uprawnienia do pracy w systemie informatycznym, może nim być pracownik lub osoba wykonująca pracę na podstawie umowy cywilnoprawnej.
9. ***Dane osobowe*** **–** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Przy czym 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.
10. ***Dane szczególnych kategorii*** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub biometryczne przetwarzane w celu

jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

11. ***Przetwarzanie*** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalenie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie usuwanie lub niszczenie.
12. ***Naruszenie ochrony danych osobowych lub incydent*** **–** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, lub nieuprawnionego dostępu do danych osobowych lub informacji przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
13. ***Informacja*** – niestanowiąca tajemnicy państwowej wiadomość, z którą zobowiązany Polityką zapoznał się w związku z wykonywaną pracą, a której ujawnienie może narazić na szkodę uzasadniony interes Uniwersytetu, interes publiczny lub prawnie chroniony interes obywateli, z wyłączeniem informacji niejawnych, których zasady ochrony normowane są odrębnie.
14. ***Zbiór danych*** **–** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
15. ***Pseudonimizacja*** – przetwarzanie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, które 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.
16. ***System informatyczny*** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

§ 3

Zasady ogólne

1. Filarami ochrony danych osobowych w Uniwersytecie są:
   1) Legalizm – Uniwersytet dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
   2) Bezpieczeństwo – Uniwersytet zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie,

3) Prawa jednostki – Uniwersytet umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,
4) Rozliczalność – Uniwersytet dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z RODO.

2. **Zasada zgodności z prawem*:***
   1) Zasada zgodności z prawem składa się z trzech pomniejszych zasad, jakimi są:
      a) legalność – oznacza zgodność dokumentacji i procedur z przepisami RODO oraz obowiązującymi ustawami i wydanymi na ich podstawie aktami wykonawczymi, a także poprzez wdrożenie odpowiednich środków organizacyjnych i technicznych do obsługi praw podmiotów danych,
      b) rzetelność – oznacza uczciwe i lojalne przetwarzanie danych w stosunku do osób, których dane dotyczą,
      c) przejrzystość – oznacza czytelną i zrozumiałą komunikację Administratora Danych z osobą, której dane dotyczą. Przejrzystość przejawia się zarówno poprzez jasne i czytelnym językiem formułowanie m.in. zgód na przetwarzanie danych i klauzul informacyjnych, jak i zrozumiałą komunikację w przedmiocie podania podstaw żądania poszczególnych danych osobowych.
   2) Przetwarzanie danych osobowych uważa się za zgodne z prawem, z zastrzeżeniem pkt 5, wyłącznie w przypadkach i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
      a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów, wzór zgody stanowi załącznik nr 1;
      b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
      c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze Danych;
      d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
      e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych.
   3) Przetwarzanie szczególnych kategorii danych osobowych uważa się za zgodne z prawem, z zastrzeżeniem pkt 5, wyłącznie w przypadkach i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
      a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach,

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora danych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile przepisy szczególne nie stanowią inaczej,
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
d) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
e) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
f) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
g) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w pkt. 4,

4) Przetwarzanie szczególnych kategorii danych osobowych do celów o których mowa w pkt 3 lit. g, może odbywać się pod rygorem zachowania tajemnicy zawodowej i na odpowiedzialność pracownika przetwarzającego te dane.
5) Administrator Danych w każdym przypadku jest w stanie wykazać, że posiada zgodę o której mowa w pkt 2 lit. a oraz pkt 3 lit. a, wyrażoną zarówno w formie pisemnej, jak i elektronicznej.

3. **Zasada celowości:**
   1) Zbieranie danych osobowych powinno być dokonywane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
   2) Niedopuszczalne jest pominięcie albo zatajenie jakiegokolwiek z celów, do którego będą przetwarzane dane osobowe.
   3) Cele przetwarzania nie mogą być podane w sposób ogólnikowy.
   4) Istnieje generalny zakaz przetwarzania danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane.
   5) W przypadku, gdy wyniknie potrzeba przetwarzania danych w nowym celu niż dotychczas, należy o nim poinformować w trybie o którym mowa w § 4 ust. 1 i upewnić się, że istnieje do niego podstawa prawna.

6) Dalsze przetwarzanie danych osobowych lub szczególnych kategorii danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych uznawane jest za operacje przetwarzania zgodne z prawem i z pierwotnymi celami, jednak z poszanowaniem zasady adekwatności wyrażonej w ust. 4.

4. **Zasada adekwatności (minimalizacji, proporcjonalności):**
   1) Zbierane dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych.
   2) Adekwatność danych powinna być oceniana najpóźniej w momencie ich zbierania.
   3) Zbieranie danych, które nie są potrzebne, ale mogą być użyteczne w przyszłości jest niedopuszczalne.
5. **Zasada prawidłowości (poprawności):**
   1) Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane.
   2) Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Tym samym przetwarzane dane muszą być aktualne i zgodne z prawdą.
   3) Administrator Danych umożliwia realizacje prawa do sprostowania i aktualizacji danych.
6. **Zasada ograniczenia czasowego (retencji danych):**
   1) Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to wyrażone w przepisach powszechnie obowiązujących lub aktach wewnętrznych, z zastrzeżeniem pkt 3.
   2) W przypadku, gdy przepisy odrębne nie ustanawiają okresu przechowywania, przechowywanie następuje według własnej oceny z zachowaniem odpowiedniej równowagi między prawami jednostki wynikającymi z obowiązujących przepisów a własnymi potrzebami związanymi z przetwarzaniem danych i osiągnięciem określonych celów przetwarzania, z zastrzeżeniem pkt 3.
   3) Dopuszcza się możliwość wyłączenia spod zasady czasowości przechowywanie danych w formie umożliwiającej identyfikację przez czas dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, jednak z poszanowaniem zasady adekwatności wyrażonej w ust. 4.
7. **Zasada bezpieczeństwa (integralności, poufności, dostępności i odpowiedniości danych):**
   1) Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub

wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2) Administrator Danych identyfikuje ryzyka naruszenia praw lub wolności osób fizycznych przy procesach przetwarzania danych osobowych w Uniwersytecie, o których mowa w ust. 1 oraz § 1 ust. 9, a także dokonuje oceny skutków ich przetwarzania zgodnie z przepisami RODO.
3) Środki techniczne i organizacyjne, o których mowa w pkt 1, zakładają m.in.:
   a) pseudonimizację i szyfrowanie danych osobowych,
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   d) regularne testowanie, mierzenie i ocenianie skuteczności tych środków.
4) Procedury postępowania opisane w niniejszym dokumencie mają zapewnić odpowiedni stopień bezpieczeństwa danych osobowych gwarantując ich:
   a) integralność, czyli właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   b) poufność, czyli właściwość zapewniająca, że dane osobowe i informacje nie są udostępniane nieupoważnionym podmiotom;
   c) dostępność, czyli właściwość zapewniająca, że dane osobowe dostępne są w danym czasie osobom upoważnionym.

8. **Zasada domyślnej ochrony danych i ochrony danych w fazie projektowania:**
   1) Z uwzględnieniem zasad wymienionych w niniejszym paragrafie, Administrator Danych zapewnia, że w Uniwersytecie realizowana jest domyślna ochrona danych, co oznacza że domyślnie przetwarzane są tylko te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Domyślna ochrona danych osobowych odnosi się do następujących obszarów:
      a) ilości zbieranych danych osobowych,
      b) zakresu przetwarzania danych osobowych,
      c) okresu przechowywania danych osobowych,
      d) dostępności do danych osobowych,
      e) reglamentacji dostępu do danych.
   2) W celu skutecznej realizacji niniejszej zasady, Administrator Danych zapewnia, że już na etapie projektowania nowych procedur, pojawieniu się nowych procesów przetwarzania, wyboru nowych technologii związanych z przetwarzaniem danych osobowych, podpisywaniu nowych umów i innych podobnych sytuacji, wdroży odpowiednie środki techniczne i organizacyjne odpowiadające ryzyku naruszenia praw i wolności osób, w tym pseudonimizację i szyfrowanie, a co najmniej zweryfikuje ich przydatność.

3) Środki techniczne i organizacyjne o których mowa w pkt 2 wynikać będą z ustalonego wcześniej ryzyka, zgodnie z § 1 ust. 9.

9. **Zasada rozliczalności:**
   1) Administrator Danych zapewnia udokumentowany przebieg wdrażania przepisów o ochronie danych osobowych oraz wykazuje w ten sam sposób przestrzeganie wszystkich ciążących na nim obowiązków, zgodnie z przepisami powszechnie obowiązującymi.
   2) Gwarancją realizacji niniejszej zasady jest zwłaszcza dostosowanie systemów informatycznych w taki sposób, aby spełniały wymagania o których mowa w § 9 ust. 1 pkt 7 i 8.

§4

Obsługa praw jednostek

1. Uniwersytet spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, poprzez:
   1) przekazywanie osobom wymaganych prawem informacji przy zbieraniu danych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
   2) zapewnienie możliwości efektywnego wykonania każdego typu żądania;
   3) zapewnienie odpowiednich nakładów i procedur, aby żądania były realizowane w terminach i w sposób wymagany przez RODO;
   4) zastosowanie procedur określających tryb zgłaszania naruszeń ochrony danych i realizacji obowiązku notyfikacyjnego, zgodnie z § 10.
2. Obowiązek informacyjny o którym mowa w ust. 1 realizowany jest także wtedy, gdy:
   1) zbierane są dane o osobie z innego źródła niż ta osoba,
   2) zmieniają się cele przetwarzania danych lub dodaje się nowy cel przetwarzania,
   3) realizuje się żądanie dostępu do danych.
3. Wzór klauzuli informacyjnej stanowi załącznik nr 2.
4. Potwierdzenie tożsamości wnioskodawcy następuje w formie elektronicznej lub papierowej poprzez weryfikację co najmniej dwóch dodatkowych danych dotyczących wnioskodawcy.
5. **Dostęp do informacji:**
   1) Uniwersytet realizując prawo dostępu do informacji na wniosek osoby, której dane dotyczą, potwierdza lub zaprzecza przetwarzanie danych wnioskodawcy. W przypadku potwierdzenia, przekazuje informacje, takie jak:
      a) cele przetwarzania danych oraz podstawę prawną przetwarzania dla każdego celu,
      b) kategorie danych,
      c) odbiorcy danych osobowych lub o kategoriach odbiorców,

d) planowany okres przechowywania danych lub kryteria jego ustalania,
e) informacje o przysługujących prawach do sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu względem przetwarzania, skargi do organu nadzorczego,
f) źródło pozyskania danych – w przypadku, gdy dane nie pochodzą od osoby, której dotyczą,
g) informacje o zautomatyzowanym podejmowaniu decyzji, profilowaniu.

2) W przypadku, gdy dane osobowe przekazywane są do państwa trzeciego lub organizacji międzynarodowej (tj. poza Europejski Obszar Gospodarczy), Administrator Danych powiadamia również osoby, których dane dotyczą o zastosowanych zabezpieczeniach związanych z przekazaniem.
3) W uzasadnionych przypadkach Administrator Danych może zwrócić się do wnioskodawcy o sprecyzowanie zakresu żądania dostępu.
4) Na wniosek osoby, której dane dotyczą Administrator Danych dostarcza kopię danych podlegających przetwarzaniu realizując tym samym prawo dostępu do informacji. Za wszelkie kolejne kopie, Uniwersytet pobiera opłatę w wysokości 20 zł od kopii.
5) W uzasadnionych przypadkach, a zwłaszcza gdy wnioskodawca składa tożsame żądanie częściej niż raz na pół roku, Administrator Danych ma prawo odmówić realizacji prawa jednostki do dostępu lub kopii danych.
6) Wniosek o dostęp do danych osobowych wnioskodawcy oraz o udzielenie informacji dotyczących przetwarzania danych Administrator Danych realizuje niezwłocznie, jednak nie później niż w ciągu 30 dni od daty wpływu wniosku, przy czym w przypadku udzielenia informacji o przetwarzaniu danych osobowych wnioskodawcy, termin na pełną odpowiedź może w uzasadnionych przypadkach ulec przedłużeniu o kolejne 2 miesiące.
7) Przekazanie informacji może nastąpić zarówno w formie elektronicznej, jak i papierowej.

6. **Sprostowanie danych:**
   1) Osobie, której dane dotyczą przysługuje prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
   2) Osobie, której dane dotyczą przysługuje prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
   3) Pracownik Administratora Danych może nie dać wiary informacjom przedstawionym przez wnioskodawcę. W tym celu może zwrócić się do Inspektora Ochrony Danych o rozstrzygnięcie sporu co do sprostowania.
7. **Prawo do bycia zapomnianym:**
   1) Osobie, której dane dotyczą przysługuje prawo żądania od Administratora Danych niezwłocznego usunięcia jej danych osobowych, w przypadku gdy:

a) dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) nastąpi cofnięcie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, przy jednoczesnym braku innej podstawy prawnej przetwarzania;
c) nastąpi wniesienie sprzeciwu wobec przetwarzania przy jednoczesnym braku nadrzędnych uzasadnionych podstaw prawnych przetwarzania;
d) dane osobowe były przetwarzane niezgodnie z prawem.

2) W przypadku realizacji prawa do bycia zapomnianym, Administrator Danych ma obowiązek:
a) usunąć dane osobowe wnioskodawcy;
b) poinformowania o usunięciu odbiorców danych, jeżeli dane te zostały im przekazane;
c) domagania się usunięcia danych od innych administratorów przetwarzających te dane, gdy dane te zostały upublicznione;
d) na żądanie osoby poinformować ją o odbiorcach którym zostały przekazane dane podlegające usunięciu.

8. **Ograniczenie przetwarzania:**
1) Osoba, której dane dotyczą może żądać od Administratora Danych ograniczenia przetwarzania w następujących przypadkach:
a) osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić Administratorowi Danych prawidłowość tych danych;
b) przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystania;
c) Administrator Danych nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia czy istnieją prawnie uzasadnione podstawy po stronie Administratora Danych, nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2) Dane osobowe co do których nastąpiło ograniczenie przetwarzania można przetwarzać, w następujących przypadkach:
a) wyłącznie za zgodą osoby, której dane dotyczą;
b) w celu ustalenia, dochodzenia lub obrony roszczeń;
c) w celu ochrony praw innej osoby fizycznej lub prawnej;
d) z uwagi na ważne względy interesu publicznego.

3) Przed uchyleniem ograniczenia przetwarzania Administrator Danych informuje o tym osobę, której dane dotyczą, a która żądała ograniczenia przetwarzania danych.
4) Ograniczenie przetwarzania nie obejmuje procesu przechowywania danych osobowych.

9. **Przenoszenie danych:**
   1) Osoba, której dane dotyczą ma prawo:
      a) otrzymać w formie papierowej lub elektronicznej dane osobowe jej dotyczące, które dostarczyła Administratorowi Danych;
      b) przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora Danych.
   2) Z prawa do przenoszenia danych osoba, której dane dotyczą może skorzystać w przypadku:
      a) przetwarzania danych odbywającego się na podstawie zgody na przetwarzanie danych osobowych lub na podstawie umowy, której stroną jest wnioskodawca;
      b) przetwarzania danych w sposób zautomatyzowany.
   3) Wykonując prawo do przenoszenia danych wnioskodawca ma prawo żądania, aby dane osobowe zostały przesłane przez Administratora Danych bezpośrednio innemu administratorowi (w przypadku gdy jest to technicznie możliwe).

10. **Sprzeciw wobec przetwarzania:**
    1) Osoba której dane dotyczą ma prawo, z przyczyn związanych z jej szczególną sytuacją, z zastrzeżeniem pkt 2 wnieść sprzeciw wobec przetwarzania danych osobowych w jednym z następujących przypadków:
       a) przetwarzania niezbędnego do wykonania zadania realizowanego w interesie publicznym;
       b) przetwarzania w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych;
       c) przetwarzania niezbędnego do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych lub przez stronę trzecią.
    2) Wnioskodawca nie może skutecznie wnieść sprzeciwu wobec przetwarzania w sytuacji, gdy jego interesy lub podstawowe prawa i wolności mają charakter podrzędny nad interesami wskazanymi w pkt 1.
    3) W przypadku wniesienia sprzeciwu Administratorowi Danych nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

§ 5

Uprawnienia i odpowiedzialność

1. Administrator Danych reprezentowany przez Rektora realizuje zadania w sprawach z zakresu ochrony danych osobowych. Do najważniejszych obowiązków Administratora Danych należy:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z przepisami powszechnie obowiązującymi;
   2) zapewnienie przetwarzania danych zgodnie z prawem oraz uregulowaniami Polityki i innymi dokumentami wewnętrznymi;
   3) zapewnienie adekwatnych do zagrożeń i kategorii przetwarzanych danych osobowych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w Uniwersytecie;
   4) powołanie Inspektora Ochrony Danych;
   5) powołanie Administratorów Systemów Informatycznych;
   6) wydawanie i cofanie upoważnień do przetwarzania danych osobowych;
   7) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   8) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
   9) nadzór nad bezpieczeństwem danych osobowych;
   10) kontrola działań jednostek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   11) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
2. Tworzy się strukturę Lokalnych Administratorów Danych, którym przekazuje się – odpowiednio do zakresu realizowanych przez nich zadań statutowych – obowiązki i uprawnienia Administratora Danych w rozumieniu ust. 1 w szczególności w zakresie wydawania upoważnień do przetwarzania danych osobowych.
3. Lokalnymi Administratorami Danych są:
   1) prorektorzy w zakresie swojej właściwości;
   2) kanclerz w zakresie swojej właściwości;
   3) dziekani wydziałów;
   4) kierownicy ogólnouczelnianych i międzywydziałowych jednostek organizacyjnych powołani przez Administratora Danych.
4. Lokalny Administrator Danych jest zobowiązany dołożyć należytej staranności w celu ochrony interesów osób, których dane dotyczą zgodnie z postanowieniami Polityki.
5. Lokalny Administrator Danych zobowiązany jest również do:

1) stworzenia właściwych warunków organizacyjno-technicznych, zapewniających ochronę danych osobowych w podległej jednostce organizacyjnej;
2) gromadzenia oryginałów upoważnień do przetwarzania danych osobowych oraz przekazywania kopii pisemnych upoważnień według właściwości do Działu Kadr celem włączenia do akt osobowych lub do Działu Płac;
3) prowadzenia rejestru czynności przetwarzania, który jest zbiorem wszystkich związanych z przetwarzaniem danych działań. Wzór rejestru czynności przetwarzania stanowi załącznik nr 3.

6. Lokalny Administrator Danych odpowiedzialny jest za nadzór nad przetwarzaniem danych osobowych związanych z wykonywaniem zadań statutowych, jak również niezbędnych dla realizacji wszelkich innych przedsięwzięć podejmowanych w jednostce.
7. Lokalni Administratorzy Danych mogą wyznaczyć Pełnomocników Lokalnych Administratorów Danych, którzy bezpośrednio realizują obowiązki Administratora Danych w jednostce organizacyjnej. Powierzenie obowiązków winno być potwierdzone pisemnie, a informacja o osobie pełniącej funkcję Pełnomocnika Lokalnego Administratora Danych powinna być przekazana do Administratora Danych oraz do Inspektora Ochrony Danych.
8. Administrator danych może powołać Zespół Inspektora Ochrony Danych na wniosek Inspektora Ochrony Danych.
9. Do zadań Inspektora Ochrony Danych należy w szczególności:
   1) informowanie Administratora Danych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych powszechnie obowiązujących przepisów o ochronie danych i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania RODO, innych powszechnie obowiązujących przepisów o ochronie danych oraz Polityki, a także podejmowanie działań zwiększających świadomość personelu uczestniczącego w operacjach przetwarzania poprzez szkolenia oraz powiązane z tym audyty;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
   4) współpraca z Prezesem Urzędu Ochrony Danych, Administratorem Danych, Lokalnymi Administratorami Danych oraz z Administratorami Systemów Informatycznych.
   5) Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
10. Inspektor Ochrony Danych realizuje także zadania wynikające bezpośrednio z Polityki, w szczególności to, o którym mowa w § 10 ust. 5, a także inne zadania, które zleci mu Administrator Danych pod warunkiem, że będą związane z ochroną danych osobowych.

11. Do zadań Administratora Systemu Informatycznego należy współpraca z Inspektorem Ochrony Danych w zakresie monitoringu nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych, a także:
    1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
    2) optymalizacja wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego;
    3) konfiguracja i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem;
    4) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
    5) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego,
    6) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego;
    7) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
    8) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji poprzez analizę dokonanych naruszeń i próbę zapobiegnięciu im w przyszłości;
    9) przyznawanie na wniosek Lokalnego Administratora Danych lub Inspektora Ochrony Danych ściśle określonych praw dostępu do informacji w danym systemie;
    10) prowadzenie ewidencji użytkowników z uprawnieniami dostępu do systemów informatycznych;
    11) wnioskowanie do Administratora Danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;
    12) zarządzanie licencjami i procedurami ich dotyczącymi;
    13) prowadzenie profilaktyki antywirusowej.
12. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania RODO, Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, oraz Polityki przez Inspektora Ochrony Danych.

§ 6

Upoważnienie do przetwarzania danych

1. Do przetwarzania danych osobowych w systemie tradycyjnym i informatycznym mogą być dopuszczone osoby posiadające upoważnienie wydane przez Administratora Danych lub Lokalnego Administratora Danych.
2. Upoważnienia wydawane są:

1) pracownikom - w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych.
2) wykonawcom usług i dostawcom sprzętu lub oprogramowania - w zakresie koniecznym do realizowania danej usług lub wykonania określonych czynności w systemie.

3. Upoważnienia wydawane są na czas określony w trzech zakresach dostępu:
   a) podstawowym - przetwarzanie danych osobowych studentów i kandydatów na studia;
   b) rozszerzonym - przetwarzanie danych osobowych studentów jednostki i pracowników jednostki organizacyjnej;
   c) pełnym - przetwarzanie danych osobowych studentów i pracowników Administratora Danych.
4. Wzór upoważnienia stanowi załącznik nr 4 do niniejszego dokumentu.
5. Zakres upoważnienia do przetwarzania danych osobowych jest adekwatny do zakresu wykonywanych zadań i nie może być on szerszy niż wynika to z realizowanych czynności zleconych przez Administratora Danych.
6. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić zmiana zakresu upoważnienia do przetwarzania danych osobowych.
7. Upoważnienie wydaje się przy zatrudnianiu pracownika po odbyciu przez tę osobę szkolenia z zakresu ochrony danych osobowych oraz podpisaniu oświadczenia w którym zobowiązuje się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Tajemnica obowiązuje osobę upoważnioną przy przetwarzaniu danych osobowych, zarówno w trakcie trwania umowy, jak i po jej ustaniu. Wzór oświadczenia stanowi załącznik nr 5.
8. Przy nadaniu, zmianie lub cofnięciu upoważnienia należy dostarczyć według właściwości do Działu Kadr lub Działu Płac oświadczenie oraz stosowne upoważnienie.
9. Cofnięcie upoważnienia do przetwarzania danych następuje:
   1) wraz z rozwiązaniem stosunku łączącego go z Administratorem Danych;
   2) na wniosek Inspektora Ochrony Danych;
   3) na umotywowany wniosek bezpośredniego przełożonego;
   4) stwierdzenia zawinionego naruszenia ochrony danych osobowych.
10. Cofnięcie uprawnień do systemów informatycznych nadanych użytkownikowi następuje zgodnie z brzmieniem ust. 9.
11. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w formie papierowej lub elektronicznej, która odzwierciedla aktualny stan nadanych i odwołanych upoważnień do przetwarzania danych. Ewidencja powinna zawierać:
    1) nazwisko i imię osoby upoważnionej,

2) stanowisko,
3) datę nadania i ustania,
4) zakres do przetwarzania danych osobowych.

12. Administrator Danych zleca prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych Lokalnym Administratorom Danych.
13. Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi załącznik nr 6.
14. Lokalny Administrator Danych występuje do Administratora Systemu Informatycznego o nadanie uprawnień do systemu informatycznego osobie upoważnionej do przetwarzania danych osobowych.
15. Administrator Systemu Informatycznego rejestruje użytkownika w systemie i nadaje mu określone uprawnienia, generuje użytkownikowi tymczasowe hasło oraz wpisuje osobę w ewidencję użytkowników w formie papierowej lub elektronicznej z prawami dostępu do systemów informatycznych, która zawiera:
    1) nazwisko i imię użytkownika,
    2) stanowisko,
    3) datę nadania i ustania uprawnień,
    4) systemy informatyczne do których użytkownik uzyskał uprawnienia,
    5) poziom nadanych uprawnień,
    6) informację czy użytkownik przetwarza dane osobowe w systemie informatycznym.
16. Wzór ewidencji użytkowników z uprawnieniami do systemów informatycznych stanowi załącznik nr 7.
17. Zakres uprawnień użytkownika do systemu informatycznego jest adekwatny do zakresu wykonywanych zadań i nie może być on szerszy niż wynika to z realizowanych czynności zleconych przez Administratora Danych.
18. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić modyfikacja uprawnień nadanych użytkownikowi. Modyfikacji dokonuje Administrator Systemu Informatycznego na wniosek Administratora Danych lub Lokalnego Administratora Danych.

§ 7

Powierzenie przetwarzania danych

1. W celu powierzenia podmiotom zewnętrznym przetwarzania danych osobowych będących w posiadaniu Administratora Danych, zawierane są umowy na powierzenie przetwarzania danych osobowych. Wzór umowy stanowi załącznik nr 8.
2. Uprawnieni do zawierania umów powierzenia przetwarzania danych osobowych są Lokalni Administratorzy Danych posiadający pełnomocnictwa do zawierania umów cywilnoprawnych.

3. Osoby uprawnione do zawierania umów powierzenia przetwarzania danych osobowych, prowadzą ewidencję zawartych umów.

§ 8

Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych i informacji w systemie tradycyjnym

1. **Zabezpieczenie danych osobowych i informacji:**
   1) Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe i informacje odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek organizacyjnych.
   2) Wszystkie dane, o których mowa w ust. 1, powinny być zabezpieczone fizycznie przed osobami nieupoważnionymi oraz przechowywane w urządzeniach gwarantujących dostęp do nich wyłącznie uprawnionych pracowników, tj. przynajmniej w pomieszczeniach zamykanych na klucz, z zastosowaniem dodatkowego zabezpieczenia w postaci szafy drewnianej zamykanej na klucz lub szafy metalowej - w odniesieniu do szczególnie istotnych dla działalności Uniwersytetu danych.
   3) Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich odpowiednie zabezpieczenie.
   4) Pomieszczenia, w których przetwarzane są dane osobowe i informacje, zabezpieczone są na czas nieobecności osób zatrudnionych przy przetwarzaniu tych danych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
   5) Dostęp do kluczy do pomieszczeń, w których przetwarzane są dane osobowe i informacje, posiadają wyłącznie osoby uprawnione przez Lokalnego Administratora Danych. Przed rozpoczęciem pracy, klucze pobierane są od pracownika ochrony nadzorującego ich przechowywanie, zaś po zakończeniu pracy są one zdawane również do pracownika ochrony.

2. **Postępowanie z danymi osobowym i informacjami:**
   1) Pracownicy zobowiązani są stosować „politykę czystego biurka”. Polega ona na utrzymywaniu porządku na stanowisku pracy pod nieobecność pracownika, poprzez umieszczanie dokumentów w szafie lub szufladzie zamykanej na klucz.
   2) Dokumentacja zawierająca dane osobowe lub informacje podlega archiwizacji zgodnie z przepisami powszechnie obowiązującymi i aktami wewnątrzzakładowymi.

3) Pracownicy zobowiązani są porządkować dokumentację pod względem jej użyteczności. Polega ona na niszczeniu wszelkiej dokumentacji roboczej lub tymczasowej zawierającej dane osobowe lub informacje niezwłocznie po ustaniu celu przetwarzania. Niszczenie polega w szczególności na:
   a) trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy użyciu niszczarki lub innych skutecznych metod;
   b) anonimizacji danych osobowych i/lub ich zbiorów polegającej na pozbawieniu danych osobowych i/lub ich zbiorów cech pozwalających na identyfikacje osób fizycznych, których anonimizowane dane dotyczą.
4) Pracownicy zobowiązani są do przewożenia, przenoszenia i przekazywania dokumentów w sposób zapobiegający ich kradzieży, zagubieniu, utracie i dostępu osób nieupoważnionych.

§ 9

Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych i informacji w systemie informatycznym

1. **Zabezpieczenie systemów informatycznych przed osobami nieupoważnionymi:**
   1) Wszelkie urządzenia i nośniki zawierające dane osobowe lub informacje, takie jak serwery, komputery główne, urządzenia teletransmisyjne, szafy z nośnikami magnetycznymi zawierające kopie danych powinny być usytuowane w pomieszczeniach uniemożliwiających dostęp do nich osób nieupoważnionych.
   2) Wyłączniki oraz zabezpieczenia zasilania elektrycznego, w już użytkowanych obiektach, powinny być zabezpieczone przed dostępem osób nieupoważnionych. W obiektach nowobudowanych lub modernizowanych wymaga się zabezpieczenia tablic zgodnie z obowiązującymi przepisami nadrzędnymi.
   3) Dostęp do pomieszczeń, w których odbywa się przetwarzanie danych osobowych i informacji winien być ściśle kontrolowany poprzez stosowane zabezpieczenia organizacyjne i mechaniczne oraz zainstalowane systemy alarmowe.
   4) System informatyczny służący do przetwarzania danych osobowych i informacji zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

5) System informatyczny służący do przetwarzania danych osobowych i informacji chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
6) W przypadku zastosowania zabezpieczeń logicznych obejmują one:
   a) kontrolę przepływu informacji pomiędzy systemem informatycznym wykorzystywanym w Uniwersytecie a siecią publiczną;
   b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
7) System informatyczny służący do przetwarzania danych osobowych – z wyjątkiem systemu służącego do przetwarzania danych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – powinien zapewniać, aby możliwe było w tym systemie odnotowanie:
   a) daty wprowadzania danych osobowych do systemu, zakres wprowadzanych zmian, zakres przeglądanych danych, identyfikator użytkownika, tak aby było możliwe ustalenie kto, kiedy i w jakim zakresie pracował na danym systemie informatycznym – powyższy obowiązek nie dotyczy systemu informatycznego, do którego dostęp posiada wyłącznie jedna osoba. Powyższe odnotowania następują automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych lub zakończeniu pracy w systemie;
   b) źródła danych w przypadku zbierania danych nie od osoby, której dane dotyczą;
   c) informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie ich udostępnienia;
   d) wniesienia któregokolwiek żądania osoby, której dane dotyczą, o których mowa w § 4;
   e) sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa powyżej.
8) Administrator Danych wdraża odpowiednie środki techniczne, aby witryny internetowe za pośrednictwem których uzyskuje się zgody na przetwarzanie danych osobowych odpowiadały wymogom o których mowa w § 3 ust. 2 pkt 5.
9) W przypadku wykorzystywania do przetwarzania danych osobowych lub informacji komputerów przenośnych jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i używania, w tym stosowania środków ochrony kryptograficznej. Użytkownik komputera przenośnego

odpowiada za powierzone mu urządzenie oraz wszelkie operacje wykonywane przy jego użyciu.

10) Komputery przenośne wykorzystywane do przetwarzania danych osobowych lub informacji, po zakończonej pracy, powinny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Za właściwe zabezpieczenie przedmiotowych urządzeń odpowiedzialni są ich użytkownicy.
11) Usytuowanie urządzeń komputerowych (komputerów typu PC, drukarek) powinno uniemożliwiać dostęp do nich osób nieuprawnionych oraz wgląd do danych wyświetlanych na monitorach komputerowych.
12) W przypadku oddalenia się pracownika od stanowiska pracy należy pozostawić system w takim stanie, aby osoby nieupoważnione nie miały do niego dostępu. W tym celu konieczne jest zablokowanie ekranu komputera oraz stosowanie chronionych hasłem wygaszaczy ekranu z odpowiednim czasem nieaktywności do ich uruchomienia (nie dłuższym niż 10 minut).
13) W przypadku naprawy sprzętu komputerowego dane osobowe lub informacje należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza jednostką, w której przetwarzane są dane osobowe, po zabezpieczeniu należy je usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną do przetwarzania danych.
14) Szczególnemu nadzorowi podlegają w Uniwersytecie urządzenia umożliwiające tworzenie i przenoszenie dużych ilości danych, w tym nagrywarki DVD oraz nośniki typu pendrive, a także nośniki komputerowe zawierające dane osobowe lub informacje. Do ich ochrony i zabezpieczenia zobowiązani są wszyscy ich użytkownicy.
15) W przypadku uszkodzenia nośników komputerowych, o których mowa w pkt 13, użytkownicy zobowiązani są do ich przekazania do właściwych służb informatycznych w celu ich zniszczenia.
16) Uszkodzone nośniki komputerowe (w tym dyski twarde), zawierające dane osobowe lub informacje, powinny być fizyczne niszczone w sposób uniemożliwiający dostęp do danych osób nieupoważnionych. Do czasu zniszczenia nośniki komputerowe powinny być zabezpieczone przed dostępem osób nieupoważnionych.
17) Dopuszcza się ponowne wykorzystanie urządzeń i nośników komputerowych zawierających dane osobowe lub informacje.

18) Urządzenia i nośniki komputerowe zawierające dane osobowe i informacje, przeznaczone do ponownego wykorzystania lub przekazania innemu podmiotowi należy – przed ich wykorzystaniem lub przekazaniem – pozbawić zapisu w sposób gwarantujący trwałe usunięcie danych (za pomocą specjalistycznego oprogramowania).

2. **Kontrola dostępu do systemu informatycznego:**
   1) System informatyczny przetwarzający dane osobowe i informacje powinien być wyposażony w mechanizmy uwierzytelniania użytkowników oraz kontroli dostępu do danych. Mechanizmy te powinny być ciągle uaktywnione.
   2) Czas dostępu użytkownika do poszczególnych danych osobowych i informacji określony jest czasem wykonania zadania wynikającego z pełnionej roli.
   3) System informatyczny musi zapewniać autoryzację i rozliczalność operacji. Każde działanie w systemie informatycznym powinno być jednoznacznie przypisane do unikalnego identyfikatora.
   4) Dostęp do danych osobowych i informacji w systemie informatycznym powinien być kontrolowany. Jest on możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. Identyfikator przydzielany jest użytkownikowi na stałe. Uwierzytelnienie użytkownika następuje za pomocą indywidualnego hasła.
   5) System informatyczny powinien posiadać możliwość kontroli złożoności i długości haseł.
   6) Każde nowe lub zmienione urządzenie służące do przetwarzania danych osobowych lub informacji musi zostać zweryfikowane co do zgodności z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez Administratora Systemu Informatycznego.

3. **Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym:**
   1) Przed uruchomieniem komputera na stanowisku pracy każdy użytkownik powinien dokonać przeglądu i sprawdzenia urządzeń komputerowych pod kątem ujawnienia okoliczności wskazujących na naruszenie dostępu do tych urządzeń lub danych zawartych na nich. W przypadku stwierdzenia naruszenia, należy postępować zgodnie z § 10 ust. 2.
   2) Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła nadanego przez Administratora Systemu Informatycznego.

3) Użytkownik opuszczając stanowisko pracy powinien zwrócić szczególną uwagę na uniemożliwienie wykorzystywania systemu komputerowego przez osoby nieupoważnione, w szczególności na włączenie opcji wygaszacza ekranu po upływie ustalonego czasu nieaktywności użytkownika.
4) Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i wylogować się z sieci komputerowej. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
5) Zabronione jest podejmowanie działań mogących być zagrożeniem dla systemu informatycznego, a w tym:
   a) łamanie haseł,
   b) dokonywanie włamań na konta innych użytkowników,
   c) nieprawne uzyskiwanie dostępu do kont administracyjnych,
   d) zakłócanie działania usługi,
   e) omijanie i badanie zabezpieczeń,
   f) doprowadzanie do rozprowadzania wirusów, koni trojańskich, niechcianej poczty i innego złośliwego oprogramowania,
   g) praca na koncie innego użytkownika.
6) Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych zagrożone karą dyscyplinarną, włącznie ze zwolnieniem w trybie dyscyplinarnym.
7) Po zakończeniu pracy należy zamknąć system, wyłączyć monitor i ewentualnie drukarkę, a także zabezpieczyć stanowisko pracy, w szczególności dokumentację i wymienne nośniki danych.

4. **Wymogi dotyczące haseł:**
   1) Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.
   2) Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
   3) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
   4) Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

5) W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
6) Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła – 8 znaków,
   b) właściwa złożoność hasła – litery wielkie i małe oraz cyfry i znaki specjalne, o ile system informatyczny na to pozwala.
7) Zakazuje się stosować haseł:
   a) które użytkownik stosował uprzednio,
   b) będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
   c) analogicznych jak identyfikator,
   d) zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci, itp.,
   e) stanowiące przewidywalne sekwencje znaków, np. 12345678 lub qwertyui.
8) Zmiany hasła nie należy zlecać innym osobom.
9) W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

5. **Tworzenie i przesyłanie plików:**
   1) Nie tworzy się plików o charakterze baz danych (np. pliku excel) bez powodów.
   2) Przed wysłaniem pliku zawierającego dane osobowe należy go odpowiednio zabezpieczyć poprzez zaszyfrowanie hasłem. Hasło należy przesłać odbiorcy pliku inną drogą komunikacji.
   3) Zabrania się podłączania do służbowego sprzętu komputerowego obcych nośników danych. O znalezionym lub zgubionym wymiennym nośniku danych typu Pendrive, zawierającym dane osobowe należy powiadomić Inspektora Ochrony Danych.
   4) Zobowiązuje się pracowników do przesyłania elektronicznej korespondencji służbowej wyłącznie za pośrednictwem Uniwersyteckiej skrzynki pocztowej.
   5) W przypadku przesyłania korespondencji elektronicznej należy ukrywać listę innych odbiorców poprzez wpisywanie adresu w polu UDW lub BCC.

§ 10

Postępowanie w przypadku naruszenia ochrony danych osobowych lub bezpieczeństwa informacji

1. Do zdarzeń mogących prowadzić do naruszenia ochrony danych osobowych i informacji zalicza się m.in.:
   1) kradzież danych w każdej formie,
   2) nieumyślną lub celową modyfikację danych, zarówno w formie elektronicznej i papierowej,
   3) utratę danych,
   4) włamania do systemu poprzez programy, takie jak:
      a) wirus,
      b) koń trojański,
      c) makro,
      d) bomba logiczna,
   5) awarie sprzętu lub uszkodzenie oprogramowania,
   6) utratę zasilania powodującą przerwę w pracy systemów,
   7) zabór sprzętu lub nośników z ważnymi danymi,
   8) nieprzestrzeganie postanowień Polityki,
   9) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych, zjawiska takie jak: naturalne katastrofy, działania silnych pól elektromagnetycznych, przechwycenie transmisji danych, odczyt z monitora komputera przez osoby nieuprawnione, zauważenie śladów usiłowania lub dokonania włamania do pomieszczenia lub szafy z danymi, zauważenie elektronicznych śladów próby włamania do systemu informatycznego Uniwersytetu.
2. Każdy pracownik Uniwersytetu w przypadku pozyskania wiedzy o fakcie bezprawnego przetwarzania, ujawnienia lub nienależytego zabezpieczenia danych osobowych przed osobami nieuprawnionymi, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo wystąpienia naruszenia, o którym mowa w ust. 1, lub zasad ochrony danych osobowych, o których mowa w § 3, zobowiązany jest niezwłocznie poinformować Lokalnego Administratora Danych lub bezpośredniego przełożonego, który powiadamia niezwłocznie o zdarzeniu Lokalnego Administratora Danych.
3. Z chwilą uzyskania informacji, o której mowa w ust. 2, Lokalny Administrator Danych niezwłocznie informuje o tym Inspektora Ochrony Danych, a także:

a) podejmuje czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość,
b) podejmuje czynności zmierzające do ustalenia przyczyn zdarzenia i sprawców,
c) rozważa wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
d) zaniecha dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie zdarzenia i jego analizę, o ile to możliwe,
e) dokumentuje w formie notatki służbowej zaistniałe zdarzenie, w której wskazuje na podjęte w tej kwestii czynności.

4. Obowiązek informacyjny, o którym mowa w ust. 2 i 3, powinien zostać zrealizowany najpóźniej następnego dnia roboczego po dniu powzięcia informacji o potencjalnym lub zaistniałym naruszeniu ochrony danych osobowych.
5. Dopuszcza się możliwość przeprowadzenia postępowania wyjaśniającego przez Inspektora Ochrony Danych, przy czym po uzyskaniu informacji, o której mowa w ust. 2, w pierwszej kolejności ustala, czy zaistniałe zdarzenie skutkuje naruszeniem praw lub wolności osób fizycznych.
6. W ramach postępowania wyjaśniającego podejmowane są czynności mające na celu wyjaśnienie okoliczności danego zdarzenia, w szczególności:
   1) ustalenie czasu wystąpienia naruszenia, jego zakresu, przyczyn, skutków oraz wielkości szkód, które zaistniały;
   2) ustalenie osoby odpowiedzialnej za naruszenie;
   3) podjęcie działań w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości;
   4) wyciągnięcie konsekwencji w stosunku do osoby ponoszącej odpowiedzialność za zdarzenie, przy czym zgodnie z przepisami powszechnie obowiązującymi z tytułu przedmiotowych naruszeń możliwa jest odpowiedzialność dyscyplinarna, cywilna lub karna;
   5) zaopiniowanie czy Administrator Danych zobowiązany jest zgłosić sprawę organom ścigania.
7. W przypadku, gdy zgłoszone naruszenie wystąpiło w systemie informatycznym Inspektor Ochrony Danych może włączyć do postępowania wyjaśniającego Administratora Systemu Informatycznego.

8. Inspektor Ochrony Danych, z zastrzeżeniem ust. 7, prowadząc postępowanie wyjaśniające ma prawo do pełnej swobody działania, dostępu do dokumentów, wglądu do operacji wykonywanych w systemie informatycznym, pobierania wyjaśnień od pracowników i osób mogących mieć wpływ na wyniki postępowania. Raport zawierający wyniki postępowania wyjaśniającego Inspektor Ochrony Danych przekazuje Administratorowi Danych.
9. Administrator Danych po uzyskaniu od Inspektora Ochrony Danych informacji o stwierdzonym naruszeniu ochrony danych osobowych lub incydencie, które skutkuje naruszeniem praw i wolności osób fizycznych albo jest wysoce prawdopodobne, w terminie 72 godzin od stwierdzenia naruszenia ochrony danych zawiadamia Prezesa Urzędu Ochrony Danych.
10. Inspektor Ochrony Danych prowadzi rejestr naruszeń ochrony danych i bezpieczeństwa informacji, stanowiący złącznik nr 9.

§ 11

Postanowienia końcowe

1. Do kontroli stanu ochrony danych osobowych w jednostkach organizacyjnych Uniwersytetu uprawnieni są:
    1) Administrator Danych,
    2) Inspektor Ochrony Danych,
    3) Lokalni Administratorzy Danych,
    4) Administratorzy Systemu Informatycznego,
    5) Pracownicy upoważnieni przez osoby wymienione w pkt 1 – 4.
2. W przypadku przeprowadzenia kontroli przez Lokalnego Administratora Danych oraz stwierdzenia w czasie kontroli odstępstw od obowiązujących zasad przetwarzania danych osobowych, kontrolujący zobowiązany jest do poinformowania Inspektora Ochrony Danych o wynikach kontroli i stwierdzonych faktach oraz uzgodnienia z nim dalszego toku postępowania.
3. Uniwersytet dba o zapoznanie pracowników z Polityką i jej przestrzeganie.
4. We wszelkich sprawach związanych z interpretacją postanowień Polityki oraz przepisów powszechnie obowiązujących dotyczących ochrony danych osobowych należy zwracać się do Inspektora Ochrony Danych.

Załącznik Nr 1
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Wzór klauzuli zgody na przetwarzanie danych osobowych zwykłych

Zgoda na przetwarzanie danych osobowych zwykłych

Wyrażam zgodę na przetwarzanie danych osobowych przez Uniwersytet Warmińsko-Mazurski w Olsztynie z siedzibą przy ul. Michała Oczapowskiego 2, 10-719 Olsztyn w celu …… .

Informujemy, że Państwa zgoda może zostać cofnięta w dowolnym momencie przez dostarczenie formularza cofnięcia zgody Inspektorowi Ochrony Danych UWM, który można pobrać ze strony: www.uwm.edu.pl/daneosobowe. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie Twojej zgody przed jej wycofaniem.

……
(wyrażam zgodę)

Tylko jeżeli dotyczy

Zgoda na przetwarzanie szczególnych kategorii danych osobowych

Wyrażam zgodę na przetwarzanie szczególnych kategorii danych osobowych przez Uniwersytet Warmińsko-Mazurski w Olsztynie z siedzibą przy ul. Michała Oczapowskiego 2, 10-719 Olsztyn w celu …… .

Informujemy, że Państwa zgoda może zostać cofnięta w dowolnym momencie przez dostarczenie formularza cofnięcia zgody Inspektorowi Ochrony Danych UWM, który można pobrać ze strony: www.uwm.edu.pl/daneosobowe

Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie Twojej zgody przed jej wycofaniem.

……
(wyrażam zgodę)

Załącznik Nr 2
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Informacja o przetwarzaniu danych osobowych

I. Administrator danych osobowych:
Administratorem Twoich danych osobowych jest Uniwersytet Warmińsko-Mazurski w Olsztynie z siedzibą przy ul. Michała Oczapowskiego 2, 10-719 Olsztyn.

II. Inspektor Ochrony Danych:
Wyznaczyliśmy Inspektora Ochrony Danych, z którym możesz się skontaktować w sprawach ochrony swoich danych osobowych i realizacji swoich praw przez formularz kontaktowy na stronie: uwm.edu.pl/daneosobowe/formularz
oraz e-mail: bkw@uwm.edu.pl; nr tel.: 89-523-36-78 lub pisemnie na adres: ul. Prawocheńskiego 9, pok. 109, 10-719 Olsztyn.

III. Cele i podstawy przetwarzania:
Przykładowo: Na podstawie Twojej zgody,
- W celu zawarcia umowy (na podstawie zainteresowania naszą ofertą)
- W celu wykonania i na podstawie zawartej przez Ciebie z nami umowy (…)
- W celach rekrutacyjnych na studia,
- W celu rekrutacji do pracy

IV. Kategorie Twoich danych, które przetwarzamy:
Przykładowo: Imię nazwisko, dane identyfikacyjne, wykształcenie, publikacje, zawód, kariera, wynagrodzenie, itp.

V. Odbiorca danych:
Twoje dane osobowe możemy udostępniać następującym kategoriom podmiotów:……

VI. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych:
Nie przekazujemy Twoich danych poza teren Polski, Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego.

VII. Okres przechowywania danych:
Twoje dane przechowujemy przez okres …… .

VIII. Twoje prawa:
Przysługuje Ci:
a) prawo dostępu do wglądu do swoich danych oraz otrzymania ich kopii,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) ograniczenia przetwarzania danych,
e) prawo do wniesienia sprzeciwu wobec przetwarzania danych,
f) prawo do przenoszenia danych,
g) prawo do wniesienia skargi do organu nadzorczego,
h) prawo do cofnięcia zgody na przetwarzanie danych osobowych.

W celu realizacji swoich praw, prosimy abyś zgłosił przysługujące Tobie żądanie Inspektorowi Ochrony Danych Uniwersytetu Warmińsko-Mazurskiego w Olsztynie. Na stronie: uwm.edu.pl/daneosobowe znajdziesz przewidziane ku temu procedury.

IX. Informacja o wymogu/dobrowolności podania danych
Podanie przez Ciebie danych jest:
- wymogiem ustawowym wynikającym z ……
- warunkiem zawarcia umowy
- warunkiem wzięcia udziału w rekrutacji
- dobrowolna

Jeżeli nie podasz danych:
- możemy odmówić zawarcia umowy
- możesz utracić prawo do studiowania w Uniwersytecie Warmińsko-Mazurskim w Olsztynie
- może zostać wypowiedziana Tobie umowa o pracę
- możemy odmówić naszego świadczenia

X. Informacja o źródle danych [zastosowanie przy zbieraniu danych nie od osoby, której dane dotyczą]
Twoje dane uzyskaliśmy od …… (Twojej firmy, Twojego publicznego profilu na *LinkedIn*, z Krajowego Rejestru Sądowego, itp.).

Załącznik Nr 3
do Polityki Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie

Rejestr czynności przetwarzania - wzór

Lp.	Czynność przetwarzania	Jednostka organizacyjna	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Kategorie odbiorców	Sposób przetwarzania danych	Sposób pozyskiwania danych	Okres przechowywania danych	Nazwa współadministratora (jeżeli dotyczy)
1											
2											
3											
4											
5											

Nazwa podmiotu przetwarzającego i jego dane kontaktowe (jeżeli dotyczy)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych	Transfer do państwa trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiot)	Kategorie transferowanych danych	Podstawa prawna transferu	Dokumentacja dotycząca odpowiednich zabezpieczeń	Data ostatniej aktualizacji

Załącznik Nr 4
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Olsztyn, dnia …….

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH
Nr …….

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016r. 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, s. 1) – zwanym dalej RODO – upoważniam Panią/Pana:

……
(imię i nazwisko)

……

(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych na poziomie:

☐ podstawowym, ☐ rozszerzonym, ☐ pełnym.

a ponadto w zakresie: ……
(Jeżeli dotyczy)

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Kodeksu pracy a także wewnętrzną polityką ochrony danych osobowych Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.

Upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Uniwersytecie Warmińsko-Mazurskim w Olsztynie.

Niniejszego upoważnienia udzielam na okres od …… do …… .

……
(Podpis osoby uprawnionej do nadania upoważnienia)

Data wygaśnięcia: …….

Odwołano, dnia …….

…..……
(Podpis osoby uprawnionej do odwołania upoważnienia)

Załącznik Nr 5
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Olsztyn, dnia …….

OŚWIADCZENIE O ZACHOWANIU W TAJEMNICY DANYCH OSOBOWYCH I INFORMACJI ORAZ SPOSOBÓW ICH ZABEZPIECZENIA

W związku z dopuszczeniem do przetwarzania danych osobowych i informacji oświadczam, że:

1. Zapoznałem się i zobowiązuję się do przestrzegania obowiązków wynikających z przepisów powszechnie obowiązujących z zakresu ochronnych danych osobowych, a także regulacji wewnętrznych Administratora Danych obowiązujących w obszarze przetwarzania danych osobowych a w szczególności Polityki Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.
2. Zapewnię bezpieczeństwo przetwarzanych danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją i zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
3. Zachowam w tajemnicy dane osobowe i informacje oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie współpracy z administratorem danych, jak i po jej zakończeniu.
4. Znane mi są zasady odpowiedzialności prawnej za niezgodne z prawem przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u Administratora Danych, a także Kodeksu Pracy i Kodeksu Cywilnego.

Oświadczam, że treść niniejszego oświadczenia jest mi znana i zrozumiała, a także zobowiązuję się do jego przestrzegania.

…..……..
(Podpis osoby składającej oświadczenie)

Załącznik Nr 6
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Ewidencja osób upoważnionych do przetwarzania danych

Imię i nazwisko	Data nadania	Data ustania	Zakres do przetwarzania danych osobowych	Stanowisko

Załącznik Nr 7
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Ewidencja użytkowników z uprawnieniami do systemów informatycznych

Imię i nazwisko	Stanowisko	Systemy informatyczne, do których użytkownik ma uprawnienia	Poziom nadanych uprawnień	Czy przetwarzane są dane osobowe? (tak/nie)

Załącznik Nr 8
do Polityki Bezpieczeństwa Informacji
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

Wzór umowy powierzenia przetwarzania danych osobowych

zawarta w Olsztynie w dniu ……. r. pomiędzy:

Uniwersytetem Warmińsko-Mazurskim w Olsztynie z siedzibą przy ul. Oczapowskiego 2, 10 - 719 Olsztyn, zwanym w dalszej części umowy „**Administratorem**”**,** reprezentowanym przez:

……

a

……..(dane podmiotu który umowę zawiera), zwanym w dalszej części umowy „**Podmiotem przetwarzającym**”, reprezentowanym przez:

……

§ 1

Powierzenie przetwarzania danych osobowych

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

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane:…….. (należy podać rodzaj danych np. dane zwykłe oraz dane szczególnych kategorii, należy podać kategorię osób, których dane dotyczą oraz w jakiej są postaci np. imion i nazwisk, nr PESEL itp.).
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu :……..(należy podać cel przetwarzania danych przez podmiot przetwarzający np. realizacji umowy nr …… z dnia……..).

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem **usuwa/ zwraca** Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. Strony zobowiązują się do wzajemnej współpracy w zakresie przetwarzania danych osobowych objętych niniejszą Umową, w szczególności Strony zobowiązują się do współpracy w zakresie realizacji obowiązku udzielania odpowiedzi na zapytania osób, których dane osobowe są przetwarzane oraz wywiązywania się z obowiązków, o których mowa w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin.

§ 4

Kontrola

1. Administrator ma prawo przeprowadzenia kontroli, czy środki bezpieczeństwa, o których mowa w § 3 ust.1,spełniają umowne i ustawowe warunki. O skorzystaniu z prawa przeprowadzenia kontroli, Administrator powinien uprzedzić Podmiot przetwarzający z co najmniej 3-dniowym wyprzedzeniem kierując w tym celu do Podmiotu przetwarzającego stosowne pisemne zawiadomienie. Po otrzymaniu zawiadomienia, Podmiot przetwarzający może wystąpić z wnioskiem o przeprowadzenie kontroli w terminie szybszym niż wyznaczony.
2. Kontrolę, o której mowa w ust. 1, Administrator winien przeprowadzić mając na uwadze godziny pracy Podmiotu przetwarzającego, w sposób możliwie niezakłócający pracy.
3. Podczas kontroli, Podmiot przetwarzający zobowiązuje się udostępnić Administratorowi wszelkie dane pozwalające na ocenę adekwatności zastosowanych środków bezpieczeństwa do istniejącego ryzyka, w szczególności udostępnić: kartoteki, bazy danych itp.

4. Podmiot przetwarzający zobowiązuje się do usunięcia wszelkich uchybień stwierdzonych podczas kontroli i opisanych w pokontrolnym protokole. Usunięcie uchybień powinno nastąpić nie później niż w terminie 7 dni od zakończenia kontroli i przedstawienia przez Administratora protokołu pokontrolnego.

§ 5

Podpowierzenie danych osobowych

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Umowa o dalsze powierzenie danych osobowych może zostać zawarta wyłącznie w celu wykonania niniejszej Umowy i może obejmować jedynie te dane - ich rodzaj, zakres oraz cel przetwarzania - o których mowa w umowie zawartej z Podmiotem przetwarzającym.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot Przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego Unii Europejskiej, któremu podlega Podmiot przetwarzający. W takim przypadku, przed rozpoczęciem przetwarzania, Podmiot przetwarzający informuje Administratora o tym obowiązku, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podwykonawca, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie, a także dawać gwarancję należytego wykonania obowiązków ochrony danych osobowych.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią niniejszej Umowy, a w szczególności za udostępnienie powierzonych danych do przetwarzania osobom nieuprawnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w niniejszej Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania w ramach niniejszej Umowy danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.
3. W przypadku podjęcia przez osobę trzecią działań prawnych wobec Podmiotu przetwarzającego i/lub Administratora związanych z naruszenia zasad przetwarzania danych osobowych, Podmiot przetwarzający będzie współpracować z Administratorem w celu podjęcia stosownych kroków prawnych zmierzających w szczególności do oddalenia

bądź odrzucenia przez właściwy sąd roszczeń osoby trzeciej, wniesienia środka odwoławczego lub zawarcia ugody, jak również innych działań prawnych.

§ 7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony od ….. do …../obowiązywania umowy podstawowej nr ……..

2. Każda ze Stron może wypowiedzieć niniejszą Umowę z zachowaniem miesięcznego okresu wypowiedzenia/razem z umową podstawową nr …. z dnia ……. w przewidzianym przez nią terminie.
3. Administrator może rozwiązać niniejszą Umowę wraz z umową podstawową nr … z dnia …… ze skutkiem natychmiastowym, w przypadku gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli, o której mowa w § 4 niniejszej Umowy nie usunie ich w wyznaczonym terminie,
b) przetwarza dane osobowe niezgodnie z postanowieniami niniejszej Umowy,
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§ 8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, a które to dane są związane z niniejszą Umową (dalej zwane **„Informacjami Poufnymi”**).
2. Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy Informacji Poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie niniejszej Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów jak i z niniejszej Umowy.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do obioru, przekazywania oraz przechowywania Informacji Poufnych gwarantowały ich zabezpieczenie, w tym w szczególności zabezpieczenie danych osobowych powierzonych do przetwarzania przed dostępem osób trzeci nieupoważnionych do zapoznania się z ich treścią.

§ 9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
2. W sprawach nieuregulowanych w niniejszej Umowie zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla Administratora.

Załącznik Nr9

do Polityki Bezpieczeństwa Informacji Uniwersytetu Warmińsko-Mazurskiego

w Olsztynie

Rejestr naruszeń ochrony danych osobowych i bezpieczeństwa informacji – wzór

Lp.	Naruszenie (opis)	Data i godzina zgłoszenia podejrzenia naruszenia	Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres którego naruszenie dotyczy	Kategoria i liczba osób, których naruszenie dotyczy	Zakres danych i kategorie danych, których dotyczy naruszenie	Źródło informacji o naruszeniu	Miejsce naruszenia	Opis skutków/konsekwencji naruszenia	Opis możliwego naruszenia praw lub wolności	Okoliczności naruszenia (opis naruszenia, przyczyny, analiza zdarzenia)	Opis skutków/konsekwencji naruszenia
1												
2												
3												
4												
5												

Opis możliwego naruszenia praw lub wolności	Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania naprawcze (opis środków zastosowanych lub proponowanych do wdrożenia)	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania UODO? (data i godzina zgłoszenia, jeżeli dotyczy wyjaśnienie)	Czy poinformowano organy ścigania? (data zawiadomienia)	Czy zachodzi obowiązek poinformowania osoby/osób których dotyczy naruszenie (sposób przekazania informacji)	Monitoring działań naprawczych