Zarządzenie Nr 63/18
Rektora Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy
z dnia 12 grudnia 2018 r.

w sprawie wprowadzenia Polityki ochrony danych osobowych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy.

Na podstawie art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenie dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. U. UEL z 2016 r., poz. 119.1 z późn. zm.) zarządzam co następuje:

§ 1.

Wprowadzam Politykę ochrony danych osobowych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy, stanowiącą załącznik.

§ 2.

Zobowiązuje kierowników komórek organizacyjnych do zapoznania pracowników z dokumentem, o którym mowa w § 1.

§ 3.

Traci moc zarządzenie nr 9/11 z dnia 21 marca 2011 r. w sprawie ustalenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy zmienionego zarządzeniem nr 87/13 z dnia 11 grudnia 2013 r.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
12.12.18.
prof. dr hab. inż. Ryszard K. Pisarski

Polityka ochrony danych osobowych
w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy

Rozdział I
Przepisy ogólne, definicje i objaśnienia

§ 1.

1. **Polityka Ochrony danych osobowych** zwana dalej „Polityką" w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu danych osobowych przez PWSZ im. Witelona w Legnicy dalej zwaną „Uczelnią".
2. Celem Polityki jest:
   1) uzyskanie optymalnego i zgodnego z wymogami obowiązujących przepisów prawa systemu ochrony danych osobowych poprzez określenie zasad sposobu przetwarzania informacji zawierających dane osobowe,
   2) podniesienie poziomu świadomości pracowników Uczelni co do istoty problemu bezpieczeństwa danych osobowych,
   3) zaangażowanie pracowników Uczelni przetwarzających dane osobowe, w ich ochronę.
3. Polityka ma zastosowanie w stosunku do wszystkich postaci informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością Uczelni lub administrowanych przez Uczelnię i przetwarzanych w systemach informatycznych, tradycyjnych (papierowych) i komunikacyjnych Uczelni.
4. Ochrona danych osobowych wynikająca z Polityki jest realizowana na każdym etapie przetwarzania informacji poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalnie i adekwatnie do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.
5. System ochrony danych osobowych Uczelni składa się z następujących najważniejszych elementów:
   1) Monitorowanie zakresu przetwarzanych danych osobowych zgodnie z ogólnymi zasadami dotyczącymi przetwarzania danych osobowych,
   2) Rejestrowanie czynności przetwarzania danych osobowych - prowadzenie Rejestru Czynności przetwarzania danych osobowych,
   3) Bezpieczeństwo przetwarzania danych osobowych - dobór zabezpieczeń w oparciu o analizę ryzyka związanego z przetwarzaniem danych osobowych,
   4) Kontrolę procesu przetwarzania danych osobowych – w tym w zakresie podstaw przetwarzania, celów, udostępniania danych osobowych oraz odpowiedni dobór podmiotów przetwarzających,
   5) Realizacja praw podmiotów danych oraz obsługi praw osoby, której dane dotyczą.
   6) Monitorowanie naruszeń ochrony danych osobowych.
6. Niniejsza Polityka Ochrony Danych Osobowych stanowi jeden ze sposobów zabezpieczenia przetwarzania danych osobowych (środek organizacyjny).

§ 2.

1. Użyte w poniższych przepisach określenia oznaczają:
   1) **Uczelnia** - Państwową Wyższą Szkołę Zawodową im. Witelona w Legnicy.
   2) **Ustawa (UODO)** –ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 poz. 1000)
   3) **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 /Dz. Urz. UE.L nr 119, str. 1/.
   4) **Administrator danych osobowych (ADO)** – osobę fizyczna lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
   5) **Lokalny Administrator Danych Osobowych (LADO)** - osobę, którą Administrator zobowiązał i udzielił odpowiedniego umocowania do wykonywania określonych uprawnień i obowiązków wynikających z ogólnego rozporządzenia o ochronie danych w jego imieniu.
   6) **Inspektor Ochrony Danych (IOD)**– osobę nadzorującą przestrzeganie zasad ochrony przetwarzania danych osobowych.
   7) **Administrator systemu informatycznego (ASI)** – osobę odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach.
   8) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
   9) **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
   10) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
   11) **System tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
   12) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

13) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
14) **Login** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
15) **Hasło** - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
16) **Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem** – osobę posiadającą upoważnienie wydane przez administratora danych dopuszczoną, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.
17) **Osoba trzecia** – każdą osobę nieupoważnioną i przez to nieuprawnioną do dostępu do danych osobowych zbiorów będących w posiadaniu administratora danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez administratora danych podejmująca czynności w zakresie przekraczającym ramy jej upoważnienia.
18) **naruszenie ochrony danych osobowych** - rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
19) **incydent** - rozumie się przez to zdarzenie lub serię powiązanych ze sobą zdarzeń, które skutkują lub mogą skutkować naruszeniem ochrony danych osobowych.

2. Skróty i definicje nadane niniejszą Polityką mają zastosowanie do załączników stanowiących jej integralną część.

§ 3.

1. Dane osobowe w Uczelni przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a 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 nr 119, str.1/, zwane dalej „RODO",
   2) Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018, poz. 1000) zwana dalej „ustawą",
   3) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) – zwane dalej „rozporządzeniem",
   4) art. 22^1 § 1-5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz.U. z 2018 r., poz. 917)

i przepisów wykonawczych wydanych z upoważnienia w/w ustaw.

2. Dane osobowe w Uczelni przetwarzane są w:
   1) celach zgodnych z przepisami prawa a w szczególności ze Statutem Uczelni oraz ustawą Prawo o szkolnictwie wyższym i nauce z dnia 20 lipca 2018 r. (Dz.U. z 2018 r. poz. 1668), w szczególności dla zabezpieczania prawidłowego toku realizacji zadań edukacyjnych, dydaktycznych, naukowych, badawczych i organizacyjnych Uczelni,
   2) dla zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni, polityki personalnej oraz bieżącej obsługi stosunków pracy, studentów i innych osób wykonujących pracę na rzecz Uczelni,
   3) dla realizacji innych zadań Uczelni, w tym wykonywania zadań realizowanych w interesie publicznym, z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

Rozdział II
Bezpieczeństwo przetwarzania danych osobowych

§ 4.

1. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz przed nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Dobór środków fizycznych, technicznych, informatycznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych Uczelnia realizuje w oparciu o szacowanie ryzyka naruszenia praw i wolności osób, których dane dotyczą zgodnie z art. 32 RODO.
3. Przy doborze zabezpieczeń należy oceniać ryzyko zarówno w kontekście skutków dla osoby, której dane dotyczą w tym np. dyskryminacja, pozbawienie przysługujących praw, szkody majątkowe i niemajątkowe), jak również ryzyko w kontekście skutków dla ADO w przypadku niepodjęcia działań związanych z zapewnieniem bezpieczeństwa przetwarzania danych osobowych zgodnie z RODO.
4. Metodyka wykonywania analizy ryzyka dla bezpieczeństwa przetwarzania danych osobowych została określona w Załączniku nr 1 do niniejszej Polityki.
5. Ustalone wymagania dotyczące zabezpieczenia danych osobowych w odniesieniu do danego procesu przetwarzania danych osobowych są odnotowywane przez IOD w prowadzonym rejestrze czynności przetwarzania danych osobowych.
6. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

7. Polityka bezpieczeństwa danych osobowych przetwarzanych na Uczelni zawarta jest w Załączniku nr 2 do niniejszej Polityki.

Rozdział III
Domyślna ochrona danych osobowych oraz ochrona danych w fazie projektowania

§ 5.

1. Planowanie realizacji nowych projektów, procesów, programów (systemów), związanych z przetwarzaniem danych osobowych (konkurs, nowa strona internetowa służąca do pobierania danych, nowy system), musi uwzględniać zasady ochrony danych w fazie projektowania („privacy by desing") oraz domyślnej ochrony danych („privacy by default"). Oceny dokonuje się przed rozpoczęciem nowego projektu.
2. Dokonywanie oceny nowego projektu pod kątem ochrony danych osobowych następuje w oparciu o formularz oceny zawarty w Załączniku nr 3 do niniejszej Polityki.

Rozdział IV
Ocena skutków dla ochrony danych osobowych

§ 6.

1. W przypadku realizacji procesów przetwarzania danych osobowych przez Uczelnię, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO.
2. W prowadzonym rejestrze czynności przetwarzania danych osobowych należy wskazać procesy dla których należy przeprowadzić ocenę skutków.
3. Ocenę skutków dla ochrony danych dokonuje się na formularzu stanowiącym Załącznik nr 1 do Metodyki analizy ryzyka i DPIA.
4. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, pomimo zastosowania środków w celu jego zminimalizowania, to przed rozpoczęciem przetwarzania należy skonsultować się z PUODO. W przypadku konieczności przeprowadzenia konsultacji z organem nadzorczym IOD przygotowuje odpowiedni wniosek o konsultacje zgodnie z art. 36 RODO i kontaktuje się w tej sprawie z organem.

Rozdział V
Ogólne zasady przetwarzania danych osobowych

§ 7.

1. Uczelnia organizuje i realizuje proces przetwarzania danych osobowych z uwzględnieniem zasad, o których mowa w Motywie 39-46 RODO oraz artykule 5 ust. 1 ppkt a) – e), ust. 2 RODO.
2. Uczelnia dba o to, aby z współpracującymi podmiotami, którym powierzane są dane osobowe do przetwarzania podpisane zostały umowy powierzenia przetwarzania tych danych osobowych. W sytuacji braku powierzenia przetwarzania danych, ale dostępu podmiotu do pomieszczeń, w których przetwarzane są dane osobowe, należy w umowach z takimi podmiotami zastosować uregulowania odnoszące się do obowiązków zapewnienia poufności i tajemnicy.
3. Filarami ochrony danych osobowych w działalności Uczelni są:
   1) Legalność – Uczelnia dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
   2) Bezpieczeństwo - Uczelnia zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
   3) Prawa podmiotów danych – Uczelnia umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
   4) Rozliczalność - Uczelnia dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

§ 8.

1. Każdy pracownik Uczelni upoważniony do przetwarzania danych osobowych przetwarza je z poszanowaniem zasad przewidzianych przez przepisy prawa:
   1) Zasadą legalności – dane są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą.
   2) Zasadą zabezpieczenia procesu przetwarzania danych osobowych, poufności i integralności danych – dane są zabezpieczone przed naruszeniami zasad ich ochrony, w tym przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub z wykorzystaniem odpowiednich środków technicznych lub organizacyjnych.

3) Zasadą przestrzegania praw podmiotu danych – przestrzega się praw podmiotów danych przyznanych im na mocy postanowień RODO, w szczególności Administrator umożliwia osobom, których dane przetwarza wykonywanie swoich praw i prawa te realizuje.
4) Zasadą rozliczalności - należy dokumentować to, w jaki sposób Administrator spełnia obowiązki wynikające z RODO, aby w każdej chwili móc wykazać zgodność z przepisami.
5) Zasadą Minimalizacji – przetwarzania dokonuje się wyłącznie zgodnie z ustalonymi celami, w konkretnych celach i nie „na zapas" (minimalizacja, adekwatność); dane są zbierane w określonych, jednoznacznych i legalnych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
6) Zasadą transparentności – informowanie i komunikacja z podmiotami danych następuje jasnym, prostym i zrozumiałym językiem, w sposób przejrzysty dla osoby, której dane dotyczą.
7) Zasadą prawidłowości danych – dba się o to aby dane osobowe były prawidłowe, a w razie konieczności dane są aktualizowane; należy podjąć wszelkie rozsądne kroki w celu zapewnienia, że dane osobowe, które są niedokładne, z uwzględnieniem celów, dla których są przetwarzane były bezzwłocznie usuwane lub poprawiane;
8) Zasadą czasowości – dane osobowe w jakiejkolwiek postaci są przechowywanie w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż wynika to z obowiązujących przepisów prawa oraz konieczności przechowywania w stosunku do celów, dla których dane osobowe są przetwarzane; po tym okresie są one anonimizowane bądź usuwane.
9) Zasadą chronionego pomieszczenia – pod nieobecność osoby uprawnionej w pomieszczeniach służących przetwarzaniu danych nie mogą przebywać osoby postronne. Trwale opuszczając pomieszczenie należy zamknąć je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja). W sytuacji pozostawienia gościa/interesanta/studenta w pomieszczeniu, należy wylogować się z systemu, zablokować dostęp do komputera oraz zabezpieczyć dokumentację (np. schować do szafki/szuflady na klucz).
10) Zasadą nadzorowania kluczy - klucze do pomieszczeń powinny być w każdym czasie pod kontrolą. Użytkownicy pomieszczeń zabezpieczają klucze do biurek oraz szaf biurowych, w których przechowywane są dokumenty zgodnie z ustalonymi zasadami.
11) Zasadą czystego biurka – zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (np. pendrive, płyt CD), nie pozostawia się bez nadzoru, w miejscach łatwo dostępnych dla osób trzecich. W celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione dokumenty należy umieszczać stroną niezawierającą danych osobowych do góry, a opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty zawierające informacje inne niż informacje o charakterze jawnym w przeznaczonych do tego celu zabezpieczonych meblach biurowych: szafach, szufladach.
12) Zasadą czystego ekranu – treści wyświetlane na ekranie komputera nie są dostępne dla osób trzecich. Każde czasowe opuszczenie pomieszczenia powinno zostać poprzedzone zablokowaniem komputera. Na wszystkich urządzeniach aktywny jest wygaszasz ekranu zabezpieczony hasłem, który aktywuje się automatycznie po przekroczeniu ustalonego czasu braku aktywności. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony.
13) Zasadą czystej drukarki/kopiarki – wszystkie osoby zobowiązane są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu (dotyczy to zwłaszcza drukarek usytuowanych w miejscach ogólnie dostępnych).
14) Zasadą czystego kosza – nieprzydatne dokumenty, brudnopisy, zbędne kopie zbiorów danych, muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Zabrania się wrzucania do kosza na śmieci płyt CD/DVD oraz innych nośników, które powinny zostać zniszczone w specjalistycznych niszczarkach lub trwale niszczone w sposób uniemożliwiający odczyt danych.
15) Zasadą bezpiecznej współpracy z podmiotami zewnętrznymi - dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) w ramach których dochodzić będzie do powierzenia przetwarzania danych osobowych zawierają zapisy dotyczące bezpieczeństwa danych osobowych, w tym klauzule bezpieczeństwa o zachowaniu poufności.
16) Zasadą „uprawnionego dostępu" – przetwarzanie danych odbywać się może tylko w oparciu o formalne upoważnienie do przetwarzania danych osobowych.
17) Zasadą dostępów i przywilejów koniecznych – każda osoba upoważniona do przetwarzania danych osobowych posiada prawo przetwarzania danych osobowych, tylko takich, które są konieczne do wykonywania poleconych jej zadań.
18) Zasadą świadomości zbiorowej – wszyscy pracownicy Uczelni są świadomi konieczności ochrony danych osobowych i aktywnie uczestniczą w tym procesie.
19) Zasada indywidualnej odpowiedzialności – za bezpieczeństwo danych osobowych odpowiadają konkretne osoby, zgodnie z powierzonym im zakresem zadań.

§ 9.

1. Dane osobowe w Uczelni przetwarzane są w sposób legalny, gdy przetwarzanie następuje na ważnej podstawie prawnej w szczególności na podstawie:
   1) zgody - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów - art. 6 ust. 1 ppkt a) RODO,
   2) niezbędności do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy - art. 6 ust. 1 ppkt b) RODO – np. umowa o pracę, umowa cywilnoprawna, umowa sprzedaży,
   3) niezbędności do wypełnienia obowiązku prawnego ciążącego na ADO art. 6 ust. 1 ppkt c) RODO (np. przepisy ustawy prawo o szkolnictwie wyższym i nauce, przepisy podatkowe, rachunkowe),
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej art. 6 ust. 1 ppkt d) RODO,
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi art. 6 ust. 1 ppkt e) RODO.

§ 10.

1. Administrator jest odpowiedzialny za wykazanie zgodności przetwarzania danych osobowych przez Uczelnię. Pracownicy uczestniczący w procesach przetwarzania danych osobowych, w szczególności ci, którzy:
   1) uczestniczą w ustalaniu sposobów oraz celów przetwarzania danych osobowych,
   2) odpowiadają za bezpieczeństwo danych osobowych,
   3) są odpowiedzialni za dobór podmiotów przetwarzających,

   zobowiązani są do realizowania procesów przetwarzania danych osobowych i podejmowania decyzji z tym związanych z uwzględnieniem zasady rozliczalności.

Rozdział VI
Organizacja ochrony przetwarzania danych osobowych i odpowiedzialność

§ 11.

1. Administratorem Danych Osobowych jest Uczelnia reprezentowana przez Rektora.
2. Obowiązki wynikające z RODO, zgodnie z odrębnie ustalonym zakresem powierza się następującym osobom:
   1) Inspektorowi Ochrony Danych;
   2) zastępcom Inspektora Ochrony Danych, jeżeli zostaną wyznaczeni,
   3) LADO - Kanclerzowi,
   4) Dziekanom,
   5) Kierownikom komórek organizacyjnych Uczelni,
3. Funkcję Inspektora Ochrony Danych, w Uczelni pełni osoba powołana przez Rektora. Głównym zadaniem IOD jest informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych osobowych i doradzanie im w tej sprawie.
4. Obowiązki w zakresie zabezpieczenia systemów informatycznych sprawuje główny informatyk za pośrednictwem Administratorów systemów informatycznych, zwanymi dalej ASI.
5. Członkowie komisji powoływani w Uczelni, na podstawie zarządzenia lub wniosku organu kolegialnego, otrzymują upoważnienia do przetwarzania danych osobowych od Rektora.

§ 12.

Administrator odpowiada za wykonanie wszelkich obowiązków wynikających z RODO, a w szczególności za:
1) wyznaczenie IOD,
2) wdrożenie środków organizacyjnych, fizycznych, technicznych i informatycznych w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, w tym polityki i procedury z zakresu ochrony danych osobowych, a także może wdrożyć kodeksy postępowania zatwierdzone przez Prezesa Urzędu Ochrony Danych Osobowych,
3) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych oraz wydawanie, zmienianie i anulowanie upoważnień do przetwarzania danych osobowych,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, z zastrzeżeniem, że Administrator może wskazać podmiot bądź osobę, która będzie prowadziła taką ewidencję w jego imieniu,
5) prowadzenie rejestru czynności przetwarzania danych osobowych we współpracy z IOD, a także rejestr kategorii czynności przetwarzania w razie przetwarzania danych osobowych w imieniu i na rzecz innego administratora danych osobowych.
6) zgłaszanie bez zbędnej zwłoki (nie później niż w terminie 72 godzin po stwierdzeniu wystąpienia zdarzenia) naruszeń ochrony danych osobowych do PUODO z zastrzeżeniem sytuacji, w których jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
7) nadzór nad zapewnianiem bezpieczeństwa przetwarzania danych osobowych, w tym szacowanie ryzyka przetwarzania danych osobowych,
8) po konsultacji z IOD, dokonanie oceny skutków dla ochrony danych, w przypadku gdy dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,
9) przetwarzanie danych osobowych zgodnie z RODO i ustawami szczególnymi,
10) przeglądy i aktualizację dokumentacji przetwarzania danych osobowych,
11) wdrożenie rekomendacji i zaleceń Prezesa Urzędu Ochrony Danych Osobowych i innych organów kontrolujących w zakresie ochrony danych osobowych.

§ 13.

1. Inspektora Ochrony Danych zwany dalej „IOD" wyznacza Rektor.
2. IOD, podlega bezpośrednio Rektorowi.
3. W celu realizacji przez IOD powierzonych zadań Administrator zapewnia:
   1) właściwe i niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych przez Uczelnię;
   2) środki niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania danych, a także środki niezbędne do utrzymania jego wiedzy fachowej;
   3) niezależność IOD w zakresie wykonywanych przez niego zadań.
4. Administrator nie może odwołać ani karać IOD za wypełnianie jego zadań zgodnie z obowiązującymi regulacjami prawnymi, w tym z przyjętą dokumentacją ochrony danych osobowych.
5. Administrator niezwłocznie po wyznaczeniu IOD podaje jego dane na stronie internetowej Uczelni oraz wszystkich klauzulach informacyjnych wydawanych przez Uczelnię.

6. Administrator zawiadamia Prezesa Urzędu Ochrony Danych o każdej zmianie danych zgłoszonych zgodnie z UODO oraz o odwołaniu IOD, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.
7. IOD realizuje zadania za pośrednictwem:
   1) kierowników komórek organizacyjnych Uczelni,
   2) Dyrektora Biblioteki,
   3) Dziekanów,
   4) ASI.
8. Do zadań IOD należy nadzór nad przestrzeganiem zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych, a w szczególności:
   1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia RODO;
   4) współpraca z organem nadzorczym;
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa wart. 36 rozporządzenia RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
   6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia RODO;
   7) pomoc Administratorowi w prowadzeniu dokumentacji przetwarzania danych osobowych;
   8) przedstawianie Administratorowi propozycji aktualizacji dokumentacji przetwarzania danych osobowych;
   9) zachowanie tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z obowiązującymi przepisami;
   10) wspieranie Administratora w prowadzeniu rejestru czynności przetwarzania danych oraz w prowadzeniu rejestru kategorii czynności przetwarzania danych;
   11) prowadzenie szkoleń dla osób uczestniczących w operacjach przetwarzania danych osobowych, w tym: szkolenie wstępne pracowników przed przyjęciem do pracy oraz szkolenia organizowane w poszczególnych jednostkach organizacyjnych Uczelni, szkolenia stanowiskowe w trakcie audytów i sprawdzeń dokonywanych przez IOD;
   12) wykonywanie kontroli i audytów minimum raz w roku w wybranych komórkach organizacyjnych oraz udokumentowanie ich raportami do Administratora;
   13) kontrolowanie przestrzegania przetwarzania danych osobowych oraz prowadzenia dokumentacji przetwarzania danych Uczelni, raportowanie stanu faktycznego wraz z rekomendacjami do Administratora;
   14) monitorowanie wykonania wyników i zaleceń analizy ryzyka i oceny skutków dla ochrony danych.
9. IOD gromadzi i przechowuje dokumentację związaną z przetwarzaniem danych osobowych w siedzibie Uczelni.

§ 14.

1. Do obowiązków ASI należy:
   1) zapewnienie optymalnej ciągłości działania systemu informatycznego,
   2) nadzór nad przeprowadzanymi pracami przy naprawach, konserwacjach systemów informatycznych zawierających dane osobowe,
   3) nadawanie, zmiana i blokowanie uprawnień do systemów informatycznych w oparciu o upoważnienie nadane przez Administratora,
   4) właściwa konfiguracja systemu informatycznego zapewniająca jego bezpieczeństwo i ograniczenie dostępu do danych osobowych przez osoby nieupoważnione,
   5) monitorowanie funkcjonowania zabezpieczeń systemów informatycznych wdrożonych w celu ochrony danych osobowych,
   6) nadzór na sprawnym działaniem systemu sporządzania kopii bezpieczeństwa (lub sporządzanie przechowywanie i regularne testowanie kopii bezpieczeństwa),
   7) podejmowanie działań w przypadku wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń lub podejrzenia naruszenia np. pojawienie się wirusa w systemie (w tym niezwłoczne informowanie IOD),
   8) instalacja i konfiguracja oprogramowania na poszczególnych urządzeniach służących przetwarzaniu danych (stacjach roboczych)
   9) świadczenie pomocy technicznej (oprogramowanie i urządzenia) dla pracowników Uczelni,
   10) dokonanie okresowej weryfikacji zainstalowanego oprogramowania na stacjach roboczych poszczególnych użytkowników,
   11) instalowanie i weryfikację zabezpieczeń urządzeń mobilnych służących do przetwarzania danych osobowych,
   12) zapewnienie bezpieczeństwa sieci komputerowej,
   13) zapewnienie prawidłowej konfiguracji i działania ochrony antywirusowej,
   14) pozostałe działania przewidziane w Polityce Bezpieczeństwa zawierającej Instrukcję Zarządzania Systemami Informatycznymi.

§ 15.

1. Kierownicy, Dyrektor Biblioteki oraz Dziekani podlegają bezpośrednio Administratorowi, a w zakresie merytorycznym wykonują wytyczne IOD.
2. Do ich obowiązków należą:

1) zapoznanie podległych pracowników z podstawowymi zasadami przetwarzania danych osobowych wynikającymi z RODO, Polityki ochrony danych osobowych, Polityki bezpieczeństwa zawierającej Instrukcję Zarządzania Systemem Informatycznym w PWSZ im. Witelona w Legnicy,
2) wykonywanie zaleceń IOD oraz ASI w zakresie ochrony danych osobowych,
3) bieżące przekazywanie do IOD wszelkich zmian mających wpływ na aktualizację prowadzonych ewidencji oraz praw dostępu do przetwarzania danych osobowych w systemach tradycyjnych,
4) bieżące przekazywanie do ASI wszelkich zmian mających wpływ na aktualizację ewidencji oraz praw dostępu do przetwarzania danych osobowych w systemach informatycznych,
5) współpracę z ASI, w zakresie wdrażania i nadzorowania przestrzegania Polityki bezpieczeństwa zawierającej Instrukcję Zarządzania Systemem Informatycznym,
6) zarządzanie czynnościami przetwarzania danych osobowych w ramach zadań, realizowanych przez daną komórkę organizacyjną,
7) występowanie z wnioskami do Rektora/Kanclerza (LADO) o nadanie, zmianę lub cofnięcie upoważnienia do przetwarzania danych osobowych. Pracownika bez stosownego upoważnienia nie można dopuścić do przetwarzania danych osobowych;
8) zapoznanie podległych pracowników i innych osób (np. współpracowników) z zasadami przetwarzania i ochrony danych w danym dziale,
9) wypełnianie obowiązków dotyczących zabezpieczenia obszaru przetwarzanych danych osobowych w danej komórce organizacyjnej (np. zamykanie szaf na klucz, zamykanie drzwi na klucz, bezpieczne zakończenie sprzętu IT).
10) zgłaszanie do IOD zamiaru rozpoczęcia nowego procesu przetwarzania danych osobowych lub zmiany w czynnościach przetwarzania danych realizowanych w danej komórce organizacyjnej Uczelni,
11) w przypadku zbierania danych osobowych, konsultowanie z IOD podstaw prawnych przetwarzania danych osobowych, w tym zbierania i archiwizowania zgód osób na przetwarzanie ich danych osobowych w wymaganych przypadkach;
12) ustalanie w porozumieniu z ASI zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w danej komórce organizacyjnej Uczelni,
13) realizacja procesu udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą i ewidencjonowanie udostępnień w odrębnym rejestrze,
14) realizacja procesów związanych z powierzaniem przetwarzania danych osobowych przez Administratora - innym podmiotom - zgodnie z zawartymi umowami powierzenia przetwarzania danych osobowych,
15) dyscyplinowanie podległych pracowników za nieprzestrzeganie zasad przetwarzania danych osobowych i obowiązków wynikających z niniejszej Polityki,
16) zgłaszanie IOD wszelkich dostrzeżonych nieprawidłowości w funkcjonowaniu systemu ochrony danych osobowych, w szczególności incydentów naruszenia bezpieczeństwa danych osobowych.

§ 16.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub rażące nienależyte wykonanie zobowiązania, w szczególności przez osobę, która wobec naruszenia nie powiadomiła o tym ADO.
2. Każda osoba Upoważniona jest zobowiązana do:
   1) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz dokumentacją dotyczącą ochrony danych osobowych;
   2) przechodzenia okresowych szkoleń z obszaru ochrony danych osobowych;
   3) przetwarzania danych osobowych wyłącznie w celu i zakresie wynikającym z nałożonych obowiązków służbowych;
   4) zachowania wyjątkowej staranności przy przetwarzaniu danych osobowych, w szczególności danych wrażliwych w celu ochrony interesów osób, których dane dotyczą;
   5) stosowania określonych procedur i środków przetwarzania oraz zabezpieczania danych osobowych;
   6) podporządkowania się poleceniom IOD oraz bezpośredniego przełożonego w zakresie ochrony danych osobowych;
   7) zachowania w poufności danych osobowych;
   8) zabezpieczenia danych osobowych przed: ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub ich udostępnieniem osobom nieupoważnionym;
   9) dopilnowania, aby przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej;
   10) dopilnowania, aby przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie - zabronione jest wyrzucanie dokumentów do koszy na śmieci bez ich właściwej anonimizacji;
   11) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
   12) zachowania należytej staranności podczas przekazywania danych osobowych drogą telefoniczną (konieczność właściwej identyfikacji rozmówcy, konieczność ustalenia, czy rozmówca jest uprawniony do pozyskania danych osobowych, przekazywanie jedynie niezbędnych informacji);
   13) przesyłania danych osobowych za pomocą sieci Internet z użyciem metod kryptograficznych (szyfrowanie danych, kanały bezpiecznej transmisji) w uzasadnionych przypadkach;
   14) niewysyłania za pomocą wiadomości e-mail danych osobowych na prywatne adresy, niekopiowanie danych na inne nośniki bez uzasadnionej potrzeby służbowej;
   15) zachowania należytej ostrożności przy transporcie dokumentów oraz nośników informatycznych, zawierających dane osobowe, poza obszarem przetwarzania Uczelni,
   16) niepozostawiania dokumentów, zawierających dane osobowe na urządzeniach wielofunkcyjnych (drukowanie, kopiowanie);
   17) nieopuszczania stanowiska bez zabezpieczenia dokumentów papierowych, zawierających dane osobowe (zasada „czystego biurka") oraz bez zabezpieczania dostępu do danych przetwarzanych w systemie informatycznym (zasada „czystego ekranu");

18) informowania o zdarzeniu operacyjnym dotyczącym danych osobowych, zgodnie z obowiązującymi w tym zakresie procedurami;
19) zaprzestania przetwarzania danych osobowych po ustaniu stosunku zatrudnienia,
20) niezwłocznego informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do IOD lub ASI.
21) zgłaszania incydentów naruszenia bezpieczeństwa IOD niezwłocznie po ich wykryciu,
22) realizowania wniosków i żądań podmiotów danych zgodnie z wytycznymi IOD,
23) wykonywania poleceń merytorycznych IOD, związanych z ochroną danych osobowych, w tym przygotowywanie projektów dokumentów, notatek i raportów związanych z systemem ochrony danych osobowych przyjętym na mocy niniejszej Polityki.

Rozdział VII
Zasady dopuszczania osób do przetwarzania danych osobowych

§ 17.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające wyraźne polecenie Administratora. Administrator wydaje upoważnienie do przetwarzania danych osobowych.
2. Upoważnienia nadaje Rektor. Rektor (ADO) udziela Kanclerzowi zwanym dalej „LADO", pełnomocnictwa do nadawania upoważnień pracownikom niebędącym nauczycielami akademickimi.
3. Członkowie komisji powoływani w Uczelni, na podstawie zarządzenia lub wniosku organu kolegialnego, otrzymują upoważnienia do przetwarzania danych osobowych od Rektora.
4. Wzór wniosku o nadanie, zmianę lub cofnięcie upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 4 do Polityki.
5. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 5 do Polityki.
6. Inspektor Ochrony Danych prowadzi rejestr upoważnień nadanych przez Rektora/LADO. Wzór rejestru upoważnień stanowi załącznik nr 6 do Polityki.

§ 18.

1. Kierownicy, Dyrektor Biblioteki oraz Dziekani wnioskują o nadanie, zmianę lub cofniecie upoważnienia do przetwarzania danych osobowych pracownikom zatrudnionym w podległych im komórkach organizacyjnych Uczelni, po uprzedniej konsultacji z IOD.
2. W przypadku osoby wykonującej na podstawie umowy cywilno-prawnej usługę, w ramach której przetwarzane są dane osobowe lub osoby realizującej w Uczelni praktykę studencką, praktykę zawodową lub osoby w inny sposób związane z Uczelnią (osoba współpracująca), z pisemnym wnioskiem o nadanie upoważnienia występuje kierownik komórki organizacyjnej zlecającej usługę lub inne zadania związane z przetwarzaniem danych osobowych.
3. Przyznanie uprawnień odbywa się zgodnie z następującą procedurą:
   1) Wnioskodawca (kierownik, dyrektor, dziekan) występuje z wnioskiem do ADO/LADO o przyznanie, zmianę lub wycofanie uprawnień do przetwarzania danych osobowych (załącznik nr 4), który przekazuje do IOD,
   2) IOD na podstawie otrzymanego wniosku, któremu nadaje numer, wypełnia upoważnienie (załącznik nr 5), i w trzech egzemplarzach przekazuje do akceptacji ADO/LADO. Zaakceptowane i podpisane upoważnienie IOD wprowadza do rejestru z czego: jeden egzemplarz otrzymuje osoba upoważniona, drugi egzemplarz jest przechowywany w aktach osobowych lub dokumentacji osoby upoważnionej, trzeci egzemplarz przechowywany jest w rejestrze osób upoważnionych.
   3) w przypadku wnioskowania o uprawnienia do przetwarzania danych w systemie informatycznym, osoba określona we wniosku kierowana jest przez Wnioskodawcę do ASI celem ustalenia loginu do systemu przetwarzania danych oraz odbycia szkolenia.
4. Jeżeli osoba upoważniana (pracownik, osoba współpracująca) podlega nadającemu upoważnienie Administratorowi lub LADO bezpośrednio, upoważnienie nadaje się bez wniosku.
5. W przypadku dostępu do systemów informatycznych Uczelni, w których są przetwarzane dane osobowe, Rektor lub LADO po konsultacji z ASI może:
   1) wyrazić zgodę na nadanie uprawnień zgodnie z wnioskowanym zakresem,
   2) wyrazić zgodę na nadanie ograniczonych uprawnień zawierających się we wnioskowanym zakresie,
   3) nie wyrazić zgody na nadanie uprawnień.
6. Decyzja, o której mowa w ust. 5 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. Od decyzji LADO wnioskujący może odwołać się do Rektora. Decyzja Rektora jest ostateczna. Osoba wnioskująca przekazuje decyzję osobie uprawnianej.
7. Każda osoba upoważniona do przetwarzanych danych osobowych zostaje zapoznana z niniejszą Polityką i jej załącznikami oraz zostaje zobowiązana do jej przestrzegania, w zakresie wynikającym z realizowanych zadań. Potwierdzeniem powyższych działań jest pisemne oświadczenie o zapoznaniu się z treścią Polityki oraz zobowiązanie do stosowania zawartych w niej postanowień, którego wzór stanowi załącznik nr 7 do niniejszej Polityki.
8. Każdy użytkownik posiadający uprawnienie do przetwarzania danych osobowych w systemie informatycznym otrzymuje od ASI jednoznaczny i niepowtarzalny login do systemu.
9. Sposób uwierzytelnienia użytkownika w systemie informatycznym określa załącznik nr 2 do niniejszej Polityki. .
10. W przypadku konieczności zmiany zakresu upoważnienia (inny lub kolejny zbiór osób, inny zakres przetwarzania danych osobowych, zmiana stanowiska pracy przez pracownika) należy przedłożyć Rektorowi lub LADO nowy wniosek o nadanie upoważnienia, stosując odpowiednio zapisy § 18.
11. W przypadku nadania osobie nowego upoważnienia dla danego zbioru osób, poprzednie upoważnienie wygasa.
12. Osoba, która odbyła szkolenie podpisuje kartę szkolenia, stanowiącą załącznik nr 8 do Polityki.

§ 19.

1. Odebranie upoważnienia do przetwarzania danych osobowych może mieć miejsce, gdy:
   1) z pracownikiem została rozwiązana (zakończona) umowa o pracę,
   2) zakres obowiązków służbowych pracownika uległ zmianie, która spowodowała utratę potrzeby przetwarzania danych osobowych,
   3) osoba spowodowała swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych,
   4) istnieje uzasadniona obawa, że przetwarzanie danych osobowych przez osobę wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
2. Odebranie upoważnienia może nastąpić na wniosek:
   1) Rektora,
   2) LADO,
   3) przełożonego pracownika lub zwierzchnika osoby współpracującej,
   4) kierownika Działu Organizacji i Spraw Osobowych,
   5) Inspektora Ochrony Danych,
   6) ASI.
3. Proces odebrania upoważnienia obejmuje:
   1) przekazanie IOD pisemnego wniosku o odebranie upoważnienia (za wyjątkiem sytuacji, gdy wnioskującym jest IOD) z określeniem imienia i nazwiska pracownika oraz jego identyfikatora w systemie informatycznym (jeśli pracownik posiada dostęp do systemu informatycznego), zakresu upoważnienia, które ma zostać odebrane, a także przyczyny konieczności odebrania upoważnienia,
   2) jeśli wnioskującym jest IOD, przygotowanie przez niego pisemnej notatki zawierającej informacje wskazane w pkt. 1),
   3) w przypadku posiadania przez pracownika, któremu upoważnienie jest odbierane uprawnień do systemu informatycznego, przekazanie ASI przez IOD polecenia unieważnienia hasła, zablokowania konta użytkownika, odebrania wszelkich uprawnień do systemu. ASI winien bez zbędnej zwłoki wykonać niezbędne czynności,
   4) poinformowanie przez IOD wnioskodawcy o odebraniu pracownikowi upoważnienia do przetwarzania danych osobowych i o odebraniu (jeśli nastąpiło) uprawnień do systemu informatycznego.

§ 20.

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, podpisać oświadczenie o zachowaniu poufności oraz uzyskać upoważnienie do przebywania w w/w pomieszczeniach. Wzór oświadczenia oraz upoważnienia stanowi załącznik nr 10 do niniejszej Polityki.

Rozdział VIII
Prowadzenie rejestru czynności przetwarzania danych osobowych

§ 21.

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych zgodnie z wymaganiami art. 30 ust. 1 RODO w stosunku do danych których jest administratorem;
2. Wzór rejestru czynności jest określony w załączniku nr 11 do niniejszej Polityki.
3. Kierownicy Działów komórek organizacyjnych Administratora mają obowiązek informowania na bieżąco IOD o procesach przetwarzania danych osobowych realizowanych w swoich działach oraz o wszelkich zmianach w tych procesach, w szczególności dotyczących:
   1) celów przetwarzania danych, w tym realizowanych czynności;
   2) kategorii osób, których dane są przetwarzane;
   3) zakresów przetwarzanych danych;
   4) podmiotów przetwarzających, którym dane są powierzane;
   5) odbiorców danych, którym dane są udostępniane.

Rozdział IX
Realizacja obowiązków przy przetwarzaniu danych osobowych. Prawa podmiotów danych

§ 22.

1. Osoby odpowiedzialne w PWSZ im. Witelona za procesy, w których zbierane są dane osobowe (kierownicy komórek organizacyjnych Uczelni, Dyrektor Biblioteki, Dziekani), mają obowiązek zachowania szczególnej staranności przy ich zbieraniu, w szczególności:
   1) sprawdzać czy są spełnione podstawy prawne na pozyskiwanie danych osobowych, zgodnie z art. 6 RODO oraz art. 9 – 10 RODO;
   2) zbierać dane osobowe dla określonych, zgodnych z prawem celów realizowanych przez Administratora;
   3) zbierać dane w zakresie adekwatnym do celów w jakich dane będą przetwarzane przez Administratora,
   4) konsultować wszelkie wątpliwości związane z przetwarzaniem danych z IOD oraz ASI.

2. W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadamiać o prawie do odwołania takiej zgody.
3. Za stosowanie właściwych oświadczeń zgody przy zbieraniu danych osobowych odpowiada kierownik danej komórki organizacyjnej Uczelni. Oświadczenia dotyczące odbierania zgody na przetwarzanie danych osobowych muszą być konsultowane z IOD.
4. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO. Aktualne wzory klauzul informacyjnych są dostępne u IOD.
5. Pracownik odpowiedzialny za organizację konferencji lub innego wydarzenia w PWSZ im. Witelona w Legnicy stosuje instrukcję postępowania stanowiącą załącznik nr 12 do Polityki.
6. Za stosowanie właściwych klauzuli informacyjnych przy zbieraniu danych osobowych odpowiada Kierownik danego Działu. Klauzule informacyjne muszą być konsultowane z IOD.
7. Administrator może ustalić obowiązujące wzory klauzul informacyjnych dla poszczególnych procesów przetwarzania danych realizowanych przez Uczelnię. Wzory klauzul informacyjnych dostępne są u IOD.
8. Administrator dba o zapewnienie możliwości realizacji praw podmiotów danych. Każdej osobie, której dane osobowe są przetwarzane przez ADO przysługują prawa określone w art. 15 – 22 RODO, w tym:
    1) prawo dostępu do danych jej dotyczących;
    2) prawo do sprostowania danych;
    3) prawo do usunięcia danych;
    4) prawo do ograniczenia przetwarzania;
    5) prawo do przenoszenia danych;
    6) prawo do sprzeciwu na przetwarzanie jej danych;
    7) prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu;
    8) prawo do cofnięcia zgody na przetwarzanie danych osobowych.
9. Za rozpatrywanie złożonych do Administratora żądań w zakresie uprawnień, o których mowa w pkt 7 odpowiada Kierownik komórki organizacyjnej Uczelni, który konsultuje się w tych sprawach z IOD. IOD przyjmuje wnioski podmiotów danych, a w razie wątpliwości prosi o doprecyzowanie żądań. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą.
10. Procedura obsługi praw podmiotów danych opisana jest w Załączniku nr 13 do Polityki.

Rozdział X
Minimalizacja i retencja danych osobowych

§ 23.

1. Dane osobowe zbierane w ramach procesów realizowanych przez Uczelnię są przetwarzane przez czas określony przez właściwe przepisy prawa lub wewnętrzne przepisy Uczelni.
2. Za określenie odpowiednich czasów retencji danych osobowych w procesach przetwarzania danych przez Uczelnię odpowiada Administrator. Dane osobowe, dla których okres przetwarzania nie wynika z obowiązujących przepisów prawa i dla których nie jest możliwe określenie z góry tego okresu w wewnętrznych przepisach, są przetwarzane tak długo, jak długo istnieje jednocześnie podstawa prawna oraz cel dla ich przetwarzania.
3. Ustanie wszelkich celów przetwarzania danych (w tym archiwizacyjnych, dochodzenia roszczeń) jest równoznaczne z koniecznością usunięcia danych osobowych.
4. Dane osobowe przetwarzane wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody, jeżeli nie jest konieczne przetwarzanie danych osobowych w celu obrony lub dochodzenia roszczeń.
5. W każdej komórce organizacyjnej Uczelni co najmniej jeden raz w każdym roku kalendarzowym odbywa się weryfikacja zasobów danych osobowych prowadzonych w formie papierowej jak i elektronicznej, obejmująca:
    1) sprawdzenie, czy dane osobowe, dla których upłynął okres przechowywania wynikający z przepisów prawa lub wewnętrznych przepisów kancelaryjno-archiwalnych zostały usunięte,
    2) sprawdzenie, czy w odniesieniu do danych osobowych, których czas przechowywania nie został określony przez właściwe przepisy prawa lub wewnętrzne przepisy, nadal istnieje podstawa prawna oraz cel ich przetwarzania.
6. W przypadku ustalenia w trakcie weryfikacji, o której mowa w pkt. 5, że okres przetwarzania danych osobowych upłynął bądź nie istnieje podstawa prawna lub cel do dalszego przetwarzania danych osobowych, dane osobowe powinny zostać trwale usunięte z nośników papierowych, elektronicznych oraz systemów informatycznych.
7. Szczegółowe zasady usuwania lub anonimizacji danych w systemach informatycznych są ustalane i realizowane przez osobę wyznaczoną przez Administratora.
8. Polityka retencji danych stanowi załącznik 14 do niniejszej Polityki. Przykładowe terminy usuwania danych osobowych opisuje Rejestr Czynności Przetwarzania.

Rozdział XI
Udostępnienie i powierzenie przetwarzania danych osobowych

§ 24.

1. Osoby, które udostępniają w imieniu Administratora dane osobowe do podmiotu zewnętrznego (w formie papierowej lub elektronicznej), przed ich udostępnieniem mają obowiązek sprawdzić czy istnieje:

1) podstawa prawna do udostępnienia danych, w tym wymóg prawa dotyczący udostępnienia danych;
2) zgoda osoby na udostępnienie danych innemu podmiotowi;
3) zapis w umowie z podmiotem współpracującym, przy spełnieniu warunku, że udostępnienie nie narusza praw i wolności osoby, której dane dotyczą;
4) wniosek o udostępnienie danych od podmiotu uprawnionego, ze wskazaniem podstawy prawnej do otrzymywania danego rodzaju danych osobowych.

2. Każda sytuacja dotycząca udostępnienia danych osobowych musi być konsultowana z IOD.

§ 25.

1. W sytuacji powierzania czynności przetwarzania danych osobowych zewnętrznemu podmiotowi (podmiotowi przetwarzającemu), należy zawrzeć z nim umowę powierzenia przetwarzania danych osobowych zgodnie z art. 28 ust. 3 RODO. Wzór umowy powierzenia stanowi załącznik nr 1 do Procedury udostępniania danych.
2. Procedura udostępniania oraz powierzania przetwarzania danych zawarta jest w Załączniku nr 15 do niniejszej Polityki.

Rozdział XII
Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§ 26.

1. Naruszenie ochrony danych osobowych dotyczy danych osobowych utrwalonych w formie fizycznych nośników danych (dokumentacja) jak i w formach elektronicznych (dane osobowe wprowadzone w systemie, plikach itp.).
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

§ 27.

1. Wszyscy pracownicy, współpracownicy Uczelni oraz podmioty przetwarzające – w przypadku identyfikacji naruszenia bezpieczeństwa danych osobowych – zobowiązani są do:
   1) niezwłocznego zaprzestania przetwarzania danych osobowych,
   2) bezzwłocznego powiadomienia bezpośredniego przełożonego o stwierdzonym naruszeniu oraz
   3) bezzwłocznego powiadomienia IOD o stwierdzonym naruszeniu, podając charakter naruszenia bezpieczeństwa danych osobowych oraz podjęte działania zaradcze.
2. IOD powiadamia ADO ustnie lub pisemnie o zaistniałym incydencie.
3. IOD wspiera Administratora przy dokonaniu oceny ryzyka naruszenia praw lub wolności osób, których dane osobowe dotyczą i powiadamia Administratora o rekomendacjach co do wyników dokonanej oceny.
4. Administrator w oparciu o uzyskaną od IOD ocenę ryzyka naruszeń, decyduje o konieczności zgłoszenia naruszenia organowi nadzorczemu oraz podmiotom których dane dotyczą.
5. W przypadku podjęcia decyzji o konieczności powiadomienia o stwierdzonych naruszeniach organu nadzorczego, IOD w imieniu Administratora bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.
6. Niezależnie od dokonanego zgłoszenia naruszenia organowi nadzorczemu, Administrator w porozumieniu z IOD podejmuje decyzje o sposobie postępowania wobec zaistniałego naruszenia i osób dopuszczających się naruszeń.
7. Inspektor ochrony danych prowadzi rejestr naruszeń oraz niezbędną dokumentację dotyczącą naruszeń. Wzór ewidencji naruszeń ochrony danych osobowych stanowi załącznik nr 16 do Polityki.
8. IOD prowadzi postępowanie w sprawie incydentu zgodnie z instrukcję opisaną w Załączniku nr 17 do Polityki.
9. Zawiadomienie o naruszeniu podmiotu danych przygotowuje IOD.

Rozdział XIII
Monitorowanie RODO

§ 28.

1. W celu weryfikacji systemu ochrony danych osobowych oraz zastosowanych środków organizacyjnych, technicznych, fizycznych i informatycznych zapewniających przetwarzanie danych osobowych zgodnie z RODO, IOD dokonuje przeglądów systemu ochrony danych osobowych, zgodnie z przyjętym planem kontroli nie rzadziej niż raz w roku.
2. Monitorowanie ochrony danych osobowych prowadzone jest:
   1) na bieżąco przez IOD,
   2) poprzez audyty okresowe i doraźne (w sytuacji wystąpienia incydentów naruszenia ochrony danych) wykonywane przez IOD albo osobę wyznaczoną przez ADO,

3) podczas audytów wewnętrznych przeprowadzanych przez upoważnione podmioty.
3. IOD okresowo analizuje zgodność dokumentacji przetwarzania danych osobowych przyjętej przez Uczelnię z przepisami o ochronie danych osobowych oraz nadzoruje jej aktualizację.
4. Przykładowy Przebieg Kontroli systemu Ochrony Danych stanowi Załącznik nr 18 do Polityki.
5. Każdy pracownik Administratora, a w szczególności LADO oraz ASI mają obowiązek współpracować z IOD w zakresie okresowych przeglądów systemu ochrony danych osobowych, udzielać mu wszelkich wyjaśnień i stosować się do jego rekomendacji i poleceń związanych z przetwarzaniem danych osobowych.
6. IOD zawiadamia kierownika komórki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem rozpoczęcia sprawdzenia.
7. IOD ma prawo dostępu w sprawdzanej jednostce do wszelkich dokumentów, urządzeń informatycznych oraz systemów związanych z przetwarzaniem danych osobowych.
8. Po zakończeniu sprawdzenia IOD przygotowuje sprawozdanie, które przekazywane jest Rektorowi oraz kierownikowi sprawdzanej jednostki.
9. Sprawozdanie jest sporządzane w formie papierowej.
10. IOD przedstawia w sprawozdaniu stwierdzone w wyniku sprawdzenia uchybienia, wnioski i zalecenia mające służyć usunięciu uchybień oraz termin realizacji zaleceń.
11. Kierownik komórki organizacyjnej Uczelni ma prawo w ciągu 7 dni od daty dostarczenia sprawozdania nie przyjąć go i złożyć pisemne zastrzeżenia w sprawie wyników sprawdzenia.
12. Jeśli w ciągu 7 dni kierownik sprawdzanej jednostki nie zgłosi zastrzeżenia, uznaje się, że przyjął sprawozdanie.
13. Rektor decyduje, czy przyjąć do realizacji zalecenia IOD, czy też uwzględnić zastrzeżenia kierownika jednostki.

§ 29.

1. Kierownicy komórek organizacyjnych, w których przetwarzane są dane osobowe zobowiązani są do stałego monitorowania zagrożeń związanych z przetwarzaniem danych osobowych, w ramach ich komórki, a następnie do analizy ryzyka w tym obszarze.
2. W szczególności wzrost ryzyka przetwarzania danych może być związany z:
   1) wynikającej ze zmian w przepisach prawa konieczności wprowadzania nowych rozwiązań technicznych lub organizacyjnych w zakresie przetwarzania danych,
   2) stwierdzeniem naruszeń ochrony danych,
   3) wprowadzaniem modyfikacji procesu przetwarzania danych osobowych w określonym istniejącym zbiorze,
   4) planowaniem przetwarzania danych osobowych w nowym zbiorze,
   5) planowaniem powierzenia przetwarzania danych podmiotowi zewnętrznemu,
   6) planowaniem przyjęcia powierzenia przetwarzania danych od podmiotu zewnętrznego.
3. W przypadku stwierdzenia wzrostu ryzyka, kierownik komórki organizacyjnej w uzgodnieniu z IOD ustala, a następnie wdraża rozwiązania minimalizujące ryzyko.

Rozdział XIV
Szkolenia i odpowiedzialność

§ 30.

1. Administrator podejmuje skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji personelu w zakresie przetwarzania danych osobowych, w tym środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.
2. Administrator utrzymuje kwalifikacje wszystkich pracowników na poziomie odpowiednim dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych, w tym danych przetwarzanych w środowisku teleinformatycznym i umożliwienia właściwego korzystania ze sprzętu i systemów informatycznych.
3. Każdy pracownik/współpracownik Administratora przed przystąpieniem do pracy na zbiorach danych osobowych ADO musi zostać przeszkolony w zakresie przepisów związanych z ochroną danych osobowych.
4. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w art. 107 – 108 UODO oraz w art. 130, 266 - 269, 287 Kodeksu karnego.
5. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 4, naruszenie zasad ochrony danych osobowych, obowiązujących w Uczelni może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością na podstawie przepisów prawa pracy.
6. Zobowiązuje się pracowników do stosowania Regulaminu Ochrony Danych Osobowych stanowiącego załącznik nr 19 do niniejszej Polityki.

Rozdział XV
Postanowienia końcowe

§ 31.

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Administrator zapoznaje z treścią Polityki swoich pracowników i współpracowników.
3. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz UODO.
4. Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator.
5. Niniejsza Polityka obowiązuje od dnia jej wprowadzenia. O wszelkich zmianach Polityki i zakresie tych zmian pracownicy są informowani przez Administratora.
6. Polityka podlega regularnym przeglądom pod kątem aktualności, nie rzadziej niż 1 raz w roku.

MEDOTYKA ANALIZY RYZYKA I DPIA

1. Zasady analizy ryzyka

1.1. Państwowa Wyższa Szkole Zawodowej im. Witelona w Legnicy, dalej jako ADO określa w niniejszej Metodyce działania jakie należy podjąć w celu dokonania analizy ryzyka związanego z przetwarzaniem danych osobowych.

1.2. Obowiązującym standardem w działalności ADO jest przygotowanie się do następstw wystąpienia zagrożenia lub zagrożeń, określenie prawdopodobieństwa jego wystąpienia oraz zaplanowania działań na rzecz minimalizacji możliwości jego wystąpienia.

1.3. Procedurą analizy ryzyka objęte są wszystkie elementy działalności ADO a w szczególności te dziedziny, w których przetwarzane są dane osobowe dotyczące danych szczególnej kategorii, w tym danych o niepełnosprawności i zdrowia.

1.4. W trakcie analizy ryzyka należy wyodrębnić następujące elementy:

a) aktywa – są to wszystkie środki i narzędzia służące przetwarzaniu danych osobowych,

b) zagrożenia – są to przykłady potencjalnych naruszeń systemu,

c) skutki – są to niepożądane następstwa zrealizowania się zagrożeń w praktyce dla praw lub wolności podmiotów danych,

d) ryzyko – jest to prawdopodobieństwo, że zagrożenia się zrealizują i przyniosą konkretny, negatywny skutek dla aktywów.

1.5. Użyte pojęcia oznaczają:

a) Aktywa/Zasoby – zasobu używane przez organizację do przetwarzania danych osobowych np. sprzęt, personel, informacje (dane osobowe).

b) Identyfikowanie ryzyka – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

c) Kontekst – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.

d) Kryteria akceptacji ryzyka – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-5.

e) Kryteria oceny ryzyka - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.

f) Naruszenie ochrony danych osobowych - oznacza 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.

g) Ocena ryzyka – jest to czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.

h) Operacja przetwarzania danych osobowych - każda czynność wykonywana 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.

i) Podatność - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

j) Proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

k) Zabezpieczenie - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

m) Zagrożenie - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

2. Procedura analizy ryzyka

2.1. ADO określił i zdefiniował zagrożenia jakie występują w jego organizacji.

2.2. ADO szczególny nacisk kładzie na ochronę praw i wolności osób, których dane są przetwarzane.

2.3. ADO dostosowuje środki ochrony przetwarzania danych osobowych do skali ryzyka. Ocenia je pod kątem utraty poufności, integralności i dostępności danych, biorąc przy tym pod uwagę ich zakres, szczególne znaczenie (wrażliwość) oraz kontekst i cele przetwarzania, a tym samym także kwestie zapewniania bezpieczeństwa usług przetwarzania (niezawodność, integralność i dostępność systemu przetwarzania) oraz zapewniania autentyczności i rozliczalności danych i podmiotów uczestniczących w przetwarzaniu.

2.4. ADO, uwzględniając stan wiedzy technicznej oraz koszt wdrażania stosuje środki redukujące nieakceptowalne prawdopodobieństwo wystąpienia zagrożeń najbardziej dotkliwych oraz stosuje środki redukujące skutki ich wystąpienia.

2.5. Inwentaryzacja zasobów (aktywów) służących przetwarzaniu danych osobowych w organizacji ADO jest załącznikiem do analizy ryzyka.
2.6. Stosowane zabezpieczenia w ADO określone są w odrębnym dokumencie prowadzonym przez IOD przy współpracy z Działem Administracyjno Technicznym.
2.7. Zagrożenia są identyfikowane z uwzględnieniem odniesienia się do zasobów aktywów służących przetwarzaniu danych osobowych w organizacji ADO oraz stosowanych zabezpieczeń.
2.8. Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy.
2.9. Szacowanie ryzyka należy traktować jako proces ciągły.
2.10. Skuteczność wdrożonych środków ochrony powinna być monitorowana i doskonalona.
2.11. Uzależnienie środków ochrony przetwarzanych danych od poziomu ryzyka wymaga oszacowania ryzyka i zastosowania środków, które je wyeliminują lub zredukują do akceptowalnego poziomu, np. rezygnacja z usługi zdalnego dostępu do bazy danych osobowych.
2.12. Zasada rozliczalności wymaga, aby proces szacowania ryzyka został przeprowadzony i udokumentowany – w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki ochrony.
2.13. Zasada rozliczalności oznacza wdrożenie wewnętrznych środków (technicznych i organizacyjnych) zapewniających zgodność przetwarzania z RODO oraz pozostawania w gotowości do wykazania tej zgodności organowi nadzorczemu lub podmiotom, których dane są przetwarzane.
2.14. Przy ocenie czy stopień bezpieczeństwa danych osobowych jest odpowiedni, uwzględnia się ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie , a w szczególności w ramach analizy ryzyka należy uwzględnić konieczne jest uwzględnienie:
a) prawdopodobieństwo wystąpienia określonego zagrożenia/zdarzenia będącego naruszeniem, oraz
b) skutek i powagę tego zagrożenia/ zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą.
2.15. Do rozwiązań i działań, które mogą być wykorzystane w celu minimalizacji ryzyka naruszenia praw i wolności osób, których dane dotyczą, w kontekście zapewnienia bezpieczeństwa przetwarzanych danych przed utratą poufności, zniszczeniem, nieuprawnioną modyfikacją lub brakiem dostępności, w art. 32 ust. 1 RODO zaliczono:
a. pseudonimizację i szyfrowanie danych osobowych;
b. zarządzanie systemem w sposób zapewniający ciągłość poufności, integralności i dostępności przetwarzanych informacji;
c. zarządzanie systemem w sposób zapewniający zdolność do szybkiego przywrócenia dostępu do danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego;
d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2.16. Szacując poziom ryzyka, należy mieć na uwadze fakt, że środki zastosowane w celu zmniejszenia poziomu skutków dla jednego z czynników mogą jednocześnie powodować zwiększenie skutków dla innego. np. zastosowanie środka zmniejszającego ryzyko utraty poufności może spowodować podniesienie ryzyka utraty dostępności, jeśli zastosowany środek jest podatny na awarie.
2.17. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA) zgodnie z odrębną procedurą.
2.18. Przeprowadzenie oceny skutków dla ochrony danych (DPIA) jest wymagane zawsze wtedy, gdy poziom ryzyka określony został jako wysoki w wyniku jego szacowania przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania.
2.19. Stwierdzenie wysokiego poziomu ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, wymaga przeprowadzenia oceny skutków dla ochrony danych, podczas której należy dodatkowo uwzględnić:
a) czy operacja przetwarzania jest niezbędna,
b) czy ingerencja w prywatność związana z przetwarzaniem tych danych jest proporcjonalna do celów przetwarzania.

3. Procedura analizy ryzyka
3.1. Przy ustalaniu ryzyka naruszenia praw lub wolności ADO bierze pod uwagę:
a/ Przetwarzanie nieprawidłowych lub niepełnych danych - Przetwarzanie danych nieprawidłowych w świetle celów ich przetwarzania stanowi naruszenie art. 5 ust. 1 lit. d RODO (obowiązek zapewnienia prawidłowości danych).
b/ Nieuprawniony dostęp - W razie uzyskania dostępu do danych przez osoby nieuprawnione, naruszona zostałaby zasada integralności i poufności danych (art. 5 ust. 1 lit. f RODO) oraz obowiązek przetwarzania danych wyłącznie na polecenie administratora (art. 29 RODO).
c/ Nieuprawnione ujawnienie lub udostępnienie - Chodzi o upublicznienie lub udostępnienie danych osobowych bez podstawy prawnej.
d/ Przypadkowe lub nieuprawnione zniszczenie, utrata lub uszkodzenie danych, w przypadku przypadkowego lub nieuprawnionego zniszczenia, utraty lub uszkodzenia danych, doszłoby do naruszenia zasady integralności i poufności danych (art. 5 ust. 1 lit. f RODO).
e/ nieuprawniona modyfikacja w razie nieuprawnionej modyfikacji danych, doszłoby do naruszenia zasady prawidłowości danych (art. 5 ust. 1 lit. d RODO).

f/ Kradzież tożsamości lub oszustwo dotyczące tożsamości Kradzież tożsamości lub oszustwo dotyczące tożsamości (oraz wiążącego się z tym naruszenia prawa karnego) może nastąpić w razie nieuprawnionego dostępu do danych osobowych (naruszenia zasady zasada integralności i poufności danych, art. 5 ust. 1 lit. f RODO) lub przetwarzania danych osobowych bez podstawy prawnej (przy naruszeniu art. 6, 9 lub 10 RODO, w zależności od kategorii danych).
g/ Naruszenie zakazu dyskryminacji - Dotyczy to takiego sposobu przetwarzania danych, który może powodować naruszenie zakazu dyskryminacji osób fizycznych z uwagi na cechę, która zalicza się do danych osobowych.
h/ Szkoda finansowa Dotyczy to takiego naruszenia ochrony danych osobowych, które może spowodować szkodę finansową osoby, której dane dotyczą.
i/ Szkoda wizerunkowa - Dotyczy to takiego naruszenia ochrony danych osobowych, które może spowodować szkodę wizerunkową osoby, której dane dotyczą. Chodzi tu o taką szkodę wizerunkową, która wynika z naruszenia prawa do prywatności lub innych przepisów służących ochronie reputacji (np. art. 23 Kodeksu cywilnego).
j/ Złamanie tajemnicy zawodowej - Dotyczy to takiego naruszenia ochrony danych osobowych, które skutkuje złamaniem prawnego obowiązku zachowania tajemnicy,
k/ Wszelkie inne naruszenia praw i wolności osób fizycznych - naruszenia intymności, poczucie wstydu, naruszenie wolności myśli.

Przykładowy katalog skutków naruszenia praw lub wolności osób fizycznych

Lp.	Katalog skutków naruszenia praw lub wolności osób fizycznych, podlegający ocenie
1	Dyskryminacja
2	Kradzież tożsamości lub oszustwo dotyczące tożsamości
3	Strata finansowa osoby fizycznej
4	Naruszenie dobrego imienia osoby fizycznej
5	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową (naruszenie godności i prywatności), w tym na skutek nieuprawnionego odwrócenia pseudonimizacji
6	Uszczerbek na zdrowiu lub śmierć
7	Wszelka inna znacząca szkoda gospodarcza lub społeczna osoby fizycznej

3.2. **Dla czynności przetwarzania, należy dokonać oceny ryzyka na podstawie przyjętej metodyki nadawania wartości ocena 4-stopniowa (pomijalne, niskie, średnie, wysokie).**
Dla każdego stopnia oceny przypisana jest wartość od 1 do 4.

Kategoria skutków	Skala poziomu skutków			
	1 – pomijalne	2 – niskie	3 – średnie	4 – wysokie
Ocena skutków naruszenia praw wolności osób fizycznych	Osoba, której dane dotyczą nie będzie ponosić negatywnych skutków, bądź też dozna niewielkich niedogodności, które z łatwością pokona (np. strata czasu, drobne nieprzyjemności). Przykład: ujawnienie imion i nazwisk osób przypisanych do lekarza POZ.	Osoba, której dane dotyczą może mieć istotne niedogodności, które uda jej się przezwyciężyć pomimo pewnych trudności (dodatkowe koszty, stres, obawa, niewielkie niedogodności fizyczne).	Osoba, której dane dotyczą może być narażona na poważne skutki, które będzie w stanie z dużą trudnością odwrócić (strata pracy, pogorszenie stanu zdrowia, uszczerbek majątkowy).	Osoba, której dane dotyczą może być narażona na poważne, a wręcz nieodwracalne skutki (śmierć, długutrwałe pogorszenie zdrowia fizycznego lub psychicznego, spirala długów, brak zdolności do pracy).

3.3. Dla każdego zestawienia „czynność przetwarzania – zagrożenia - skutek" należy ocenić prawdopodobieństwo wystąpienia zagrożeń umożliwiające urzeczywistnienie się skutków. Skutki należy ocenić na podstawie przyjętej metodyki nadawania wartości np. ocena 5 stopniowa (Mało prawdopodobne, Średnio prawdopodobne, Bardzo prawdopodobne, Wysoce prawdopodobne, Niemal pewne).

Ocena prawdopodobieństwa wystąpienia zagrożenia		
Wartość (P)	**Nazwa**	**Opis**
5	Niemal pewne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie zmaterializuje się w najbliższym czasie (prawie na 90%).
4	Wysoce prawdopodobne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje. istnieje więcej niż połowa szans na wystąpienie. Materializowało się w przeciągu ostatniego roku.
3	Prawdopodobne	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa. Materializowało się w przeszłości (w ciągu ostatnich 2 lat)
2	Średnio prawdopodobne	Zagrożenie może wystąpić sporadycznie (nie przekracza 25%). Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 3 lat).
1	Mało	Zagrożenie raczej nie wystąpi lub możliwość jego
	prawdopodobne	wystąpienia jest znikoma (bliska zeru). Zagrożenie nie materializowało się w przeszłości.

3.4. Ocena powagi ryzyka (wartości oczekiwanej)
Wyliczenie poziomu Ryzyka (R) następuje poprzez iloczyn określonego przez ADO Prawdopodobieństwa (P) wystąpienia zagrożenia w ADO i Skutku (S) wystąpienia takiego zagrożenia dla podmiotów danych i ADO. Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych oblicza się na podstawie niniejszego wzoru:

$$R = S * P$$

gdzie:
R – Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania
S – Ocena skutków naruszenia praw lub wolności osób fizycznych
P – Ocena prawdopodobieństwa urzeczywistnienia się skutków
Uwaga, w kontekście ochrony danych osobowych nie priorytetyzuje się istotności czynności przetwarzania danych osobowych między sobą.

3.5. Poziom akceptacji Otrzymane wyniki powagi ryzyka naruszenia praw lub wolności osób fizycznych należy przedstawić w postaci rankingu ryzyka, czyli od największej do najmniejszej wartości. Poziom akceptacji ryzyka definiowany jest na podstawie przyjętej metodyki i wskazuje jaka wartość powagi ryzyka wymaga wdrożenia planu zaradzeniu ryzyka. Poniższe tabele przedstawiają macierz ryzyka dla prywatności i poziom jego akceptacji.

MACIERZ RYZYKA

Ocena skutków		**Ocena prawdopodobieństwa**				
		1	**2**	**3**	**4**	**5**
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15

Powaga ryzyka	Sposób postępowania (decyzję podejmuje ADO po konsultacji z IOD)
1-6	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia występują na poziomie minimalnym. Ryzyka akceptowane, niewymagające dalszego postępowania (poza cyklicznym monitorowaniem).
7-11	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia występują na poziomie średnim. Ryzyka akceptowane z użyciem określonych zabezpieczeń minimalizujących ryzyko, wymagające dalszego postępowania (poza cyklicznym monitorowaniem).
12-20	Ryzyka nieakceptowane, wymagające zastosowania postępowania z ryzykiem. Ryzyka, które powinny być kompensowane wszystkimi możliwymi zabezpieczeniami, adekwatnie do potencjalnych kosztów rekompensaty. Powinno być możliwe stałe monitorowane w całym okresie przetwarzania danych.

4. **Reakcja na ryzyko**

4.1. Jeśli ryzyko jest na poziomie akceptowalnym, ADO potwierdza jedynie, że zastosowane zabezpieczenia są właściwe.

4.2. W przypadku ryzyka na poziomie opcjonalnym ADO musi ocenić czy jest możliwość obniżenia jego poziomu poprzez zastosowanie stosownych zabezpieczeń lub czy może je zaakceptować.

4.3. W przypadku akceptacji ryzyka ADO ma obowiązek jego monitorowania.

4.4. W celu obniżenia poziomu ryzyka ADO może przeprowadzić następujące czynności:

a) przeniesienie ryzyka – np. zakup ubezpieczenia, powierzenie procesów przetwarzania podmiotom zewnętrznym,

b) unikanie ryzyka – np. poprzez modyfikację procedur, które mają na celu wyeliminowanie potencjalnie niebezpiecznych sytuacji,

c) obniżanie ryzyka – np. poprzez zastosowanie dodatkowych zabezpieczeń,

4.5. W przypadku, kiedy ryzyko jest na poziomie nieakceptowalnym, ADO po wprowadzeniu dodatkowych zabezpieczeń, przeprowadza ponowną analizę ryzyka.

5. Ocena skutków dla ochrony danych (DPIA)

5.1. Ocena skutków dla ochrony danych - (DPIA – Data Protection Impact Assesment) – nałożony przez RODO obowiązek analizy w jaki sposób operacja przetwarzania danych osobowych (planowana a także już prowadzona) wpływa lub będzie wpływać na prawa i wolności osób, których dane są przetwarzane w ramach danej operacji przetwarzania.

5.2. DPIA stosowana jest dla operacji przetwarzania danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. ADO monitoruje wskazówki PUODO w zakresie wydawanych rekomendacji dotyczących czynności wymagających dokonania DPIA.

5.3. Ocena skutków dla ochrony danych w praktyce przeprowadzana będzie dla wszelkich przedsięwzięć (np. projektów, zakupów urządzeń i nowych technologii) i procesów, podczas których przetwarzane są lub będą dane osobowe i z tym przetwarzaniem wiąże się ryzyko (obecnie lub w przyszłości) naruszenia praw i wolności osób fizycznych.

5.4. Operacje przetwarzania danych osobowych w ADO mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, gdy:

a) Przetwarzane są dane osobowe wrażliwe oraz o charakterze wysoce osobistym,

b) Dane osobowe przetwarzane są na dużą skalę,

c) Przetwarzane są dane o stanie zdrowia,

d) Monitoruje się zachowania osób fizycznych na dużą skalę,
e) ADO dokonuje systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
f) Dany proces przetwarzania znajduje się na liście rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony publikowanej przez PUODO.
5.5. O konieczności przeprowadzania DPIA decyduje ADO po zasięgnięciu opinii u prawnika lub IOD, gdy jest powołany.

6. Naruszenie praw i wolności
6.1. Definicja naruszenia praw i wolności jest bardzo szeroka i ma charakter otwarty. Szczegółowe odniesienie się do zagrożeń w tej materii znajduje się w Motywie 75 RODO, ale wszystkie łączne przesłanki sprowadzają się do prawa do prywatności osób, których dane przetwarzamy.
6.2. W ADO dodatkowo należy brać pod uwagę prawa osób, których dane są przetwarzane z perspektywy praw przysługujących im jako konsumentom.
6.3. Oceniając naruszenie praw i wolności należy odnieść się do szkód fizycznych oraz strat o charakterze materialnym i niematerialnym dla osób fizycznych.

7.Odpowiedzialność za przeprowadzenie DPIA
7.1. Za przeprowadzanie DPIA oraz wszelką weryfikację konieczności jej przeprowadzania odpowiedzialność ponosi ADO. ADO obok IOD wyznacza dodatkowo pracownika, który będzie odpowiadał za realizację DPIA w kwestiach merytorycznych, jednak odpowiedzialność za brak lub niewłaściwe przeprowadzenie DPIA ponosi ADO.
7.2. Ostateczna decyzja co do konieczności przeprowadzenia DPIA spoczywa na ADO.
7.3. ADO może również zasięgnąć opinii innych podmiotów, stowarzyszeń lub dokonać pytań ankietowych w kwestii oceny skutków dla ochrony danych wśród osób, których dane osobowe są przetwarzane.
7.4. Wszelkie czynność związane z przeprowadzaniem DPIA lub oceną konieczności jej przeprowadzenia są dokumentowane i odbywają się pisemnie.
7.5. Jeżeli zasięga się opinii innych osób, w tym pracowników w zakresie DPIA musi pozostawić im rozsądny termin, nie krótszy niż 5 dni roboczych, na przekazanie przez nich pisemnej opinii.

8. Elementy DPIA
8.1. Ocena wpływu na ochronę danych osobowych zawiera co najmniej następujące elementy:
a) Systematyczny opis planowanej operacji przetwarzania danych osobowych
b) Ocenę niezbędności i proporcjonalności przetwarzania danych w stosunku do celów przetwarzania,
c) Analizę i ocenę ryzyka w odniesieniu do potencjalnego naruszenia praw i wolności osób fizycznych wraz ze środkami minimalizującymi to ryzyko oraz uzasadnieniem dokonanego wyboru środków,
d) Określenie uczestników procesu DPIA,
e) Wyniki konsultacji z Inspektorem ochrony danych,
f) Opinie osób, których dane dotyczą lub ich przedstawicieli, gdy ich zasięgnięto.

9. Sposób wypełnienia Formularza oceny DPIA
9.1. Formularz Oceny DPIA składa się z następujących elementów:
1) szczegółowego opisu operacji przetwarzania oraz zastosowanych środków ochrony
2) oceny niezbędności i proporcjonalności środków ochrony
3) oceny oraz zarządzania ryzykiem i matrycy ryzyka

9.2. Szczegółowy opis operacji przetwarzania oraz zastosowanych środków ochrony zawiera:
1) szczegółowy opis Nowego Projektu/Procesu,
2) opis zasobów wykorzystywanych do przetwarzania danych osobowych,
3) wskazanie organizacyjnych środków ochrony danych osobowych,
4) wskazanie fizycznych oraz technicznych środków ochrony danych osobowych.

9.3. Opis środków przyczyniających się do zgodności przetwarzania z ogólnymi zasadami Rozporządzenia:
1) należy opisać środki organizacyjne, informatyczne i techniczne, które mają mieć zastosowanie w ramach Projektu przetwarzania danych osobowych (opis planowanych środków),
2) planowane środki podlegają ocenie IOD i w przypadku uznania, że nie gwarantują one zgodności z zasadami ogólnymi Rozporządzenia, IOD formułuje zalecenia dotyczące wdrożenia dodatkowych środków,
3) dokonując oceny, IOD może posiłkować się wynikami szacowania ryzyka zgodnie z niniejszą Metodyką (z art. 32 RODO),
4) w przypadku decyzji o braku wdrożenia zalecanych środków, powinien on swoją decyzję uzasadnić i wskazać powody, dla których nie wdrożono zalecanych środków oraz załączyć do tego formularza opinię IOD w tym zakresie. Opinia IOD powinna zostać sporządzona na piśmie i przekazana w formie papierowej lub elektronicznej.

9.4. Opis środków przyczyniających się do zachowania praw osób, których dane osobowe dotyczą składa się z co najmniej odpowiedzi na zamieszczone w arkuszu pytania i konsultacji z IOD. IOD w przypadku uznania, że nie gwarantują one praw osób, których dane dotyczą, IOD formułuje zalecenia dotyczące wdrożenia dodatkowych środków, Postanowienie pkt 9.6. ppkt 3-4 stosuje się odpowiednio.

9.5. Ocena ryzyka zawiera:

1) opis zagrożeń mających wpływ na stopień ryzyka naruszenia prywatności,
2) ocenę ryzyka,
3) ocenę w zakresie konsultacji z Organem nadzorczym oraz podmiotami danych,

9.6. Opis zagrożeń mających wpływ na stopień ryzyka naruszenia prywatności wchodzi w skład listy zagrożeń, które mogą wystąpić w związku z realizacją Projektu.

9.7. Ocena ryzyka dokonywana jest na podstawie dwóch kryteriów, kryterium Skutki (wagi) Zagrożenia oraz kryterium Prawdopodobieństwa wystąpienia Zagrożenia:

1) osoba dokonująca oceny powinna- w zakresie każdego wskazanego Zagrożenia - przypisać wartość dla Skutki (1 - 5) oraz Prawdopodobieństwa (1 - 5),
2) wartość dla Skutki należy ustalić biorąc pod uwagę skutki, które może spowodować wystąpienie konkretnego Zagrożenia dla praw i wolności podmiotów danych,
3) wartość dla Prawdopodobieństwa należy ustalić, biorąc pod uwagę możliwość wystąpienia konkretnego Zagrożenia, przy uwzględnieniu środków organizacyjnych, fizycznych oraz technicznych, które zostały wdrożone przez PWSZ lub są objęte planem wdrożenia przed rozpoczęciem Projektu,
4) wartość dla Skutki ustalona dla danego Zagrożenia nie może ulec zmianie w wyniku wdrożenia środków ochrony (jest to wartość stała),
5) wartość dla Prawdopodobieństwa ustalona dla danego Zagrożenia może ulec zmianie w wyniku wdrożenia środków ochrony,
6) stopień potencjalnego ryzyka stanowi iloczyn wartości dla Skutki oraz Prawdopodobieństwa,

Przyjmuje się następujące Stopnie potencjalnego ryzyka:

a) Niski - gdy iloczyn mieści się w przedziale 1-5,
b) Średni - gdy iloczyn mieści się w przedziale 6-15,
c) Wysoki - gdy iloczyn mieści się w przedziale 16-25

9.11. Zalecenia dotyczące środków służących do minimalizacji zagrożenia dla bezpieczeństwa danych osobowych (środki minimalizujące ryzyko):

1) w przypadku, gdy dla danego Zagrożenia Stopień ryzyka potencjalnego został ustalony na poziomie Wysokim, osoba dokonująca oceny DPIA powinna zwrócić się do IOD o sformułowanie zaleceń dotyczących środków minimalizujących ryzyko. W razie potrzeby osoba dokonująca oceny DPIA może zasięgnąć także opinii Działu Administracyjno Technicznego lub Radcy Prawnego.
2) w przypadku, gdy dla danego Zagrożenia Stopień ryzyka potencjalnego został ustalony na poziomie Średnim, zalecane jest aby osoba dokonująca oceny DPIA zwróciła się do IOD o sformułowanie zaleceń dotyczących środków minimalizujących ryzyko. W razie potrzeby Inicjator może zasięgnąć także opinii Działu Administracyjno Technicznego lub Radcy Prawnego.
3) w przypadku, gdy dla danego Zagrożenia Stopień ryzyka potencjalnego został ustalony na poziomie Niskim, ADO nie jest zobowiązana do wdrożenia środków minimalizujących ryzyko,
4) w przypadku decyzji o braku wdrożenia zalecanych środków, pomimo ustalenia stopnia ryzyka potencjalnego na poziomie Średnim lub Wysokim, należy tę decyzję uzasadnić oraz załączyć opinię IOD w tym zakresie. Opinia IOD powinna zostać sporządzona na piśmie i przekazana w formie papierowej lub elektronicznej.

9.12. Wartość dla Prawdopodobieństwa należy ustalić po uwzględnieniu środków ochrony, które zostały wdrożone w związku z zaleceniami dotyczącymi środków minimalizujących ryzyko oraz środków, co do których została podjęta decyzja o ich wdrożeniu przez rozpoczęciem realizacji Inicjatywy.

9.13. Ocena w zakresie konsultacji z Organem nadzorczym oraz podmiotami danych:

1) Konsultacje z Organem nadzorczym:

a) W przypadku, gdy Stopień ryzyka jest Wysoki, ADO ma obowiązek skonsultować się z Organem nadzorczym i przekazać sprawę dla IOD,

b) IOD powinien opisać wynik konsultacji,

c) w przypadku wdrożenia dodatkowych środków IOD uwzględnia je w opisie operacji przetwarzania. Decyzję co do wdrożenia dodatkowych środków podejmuje Administrator. W przypadku podjęcia decyzji o braku wdrożenia zalecanych środków, należy tę decyzję uzasadnić oraz załączyć opinię IOD w tym zakresie. Opinia IOD powinna zostać sporządzona na piśmie i przekazana w formie papierowej lub elektronicznej.

2) Konsultacje z podmiotami danych: w przypadku, gdy Stopień ryzyka szczątkowego jest Wysoki, osoba dokonując oceny ma obowiązek skonsultować się z IOD w celu dokonania oceny, czy istnieje uzasadnienie dla zasięgnięcia opinii podmiotów danych lub ich przedstawicieli zgodnie z art. 35 ust. 9 Rozporządzenia 2016/679. Opinia IOD powinna zostać sporządzona na piśmie i przekazana w formie papierowej lub elektronicznej. Osoba dokonująca oceny powinna opisać wynik konsultacji oraz zalecenia w zakresie wdrożenia środków ochrony.

Załączniki:

1. Formularz - Ocena skutków dla ochrony danych (DPIA)
2. Analiza ryzyka

FORMULARZ DPIA OCENY SKUTKÓW PRZETWARZANIA DLA OCHRONY DANYCH

I - SZCZEGÓŁOWY OPIS OPERACJI PRZETWARZANIA ORAZ ZASTOSOWANYCH ŚRODKÓW OCHRONY

	PYTANIE	ODPOWIEDŹ
	Opis operacji oraz charakteru przetwarzania danych (należy m.in. wskazać, czy zachodzi profilowanie lub zautomatyzowane podejmowanie decyzji)	
	Cele przetwarzania danych osobowych	Chodzi o cel którego realizacji podporządkowany jest cały proces. Jeśli występuje więcej niż jeden cel, należy zidentyfikować je jako odrębne procesy przetwarzania danych. W odniesieniu do już funkcjonujących procesów, cel podany jest w rejestrze czynności przetwarzania. W odniesieniu do istniejących procesów, odpowiedź należy skopiować z opisu czynności przetwarzania. Należy zbadać, czy do analizowanego procesu przyporządkowany jest tylko jeden cel przetwarzania. W razie wielu celów przetwarzania, należy zidentyfikować je jako odrębne procesy (1 cel = 1 proces).
	Czy dane są przetwarzane dalej w innych celach? Jeśli tak, w jakich?	W braku zgody lub szczególnego przepisu prawnego, które umożliwiają przetwarzanie danych w celach innych, niż zostały zebrane, do oceny zgodności dalszego przetwarzania z pierwotnym celem należy wykorzystać następujące kryteria:
	Podstawy prawne przetwarzania danych osobowych (w tym profilowania oraz automatycznego podejmowania decyzji)	Należy wskazać, w jakim zakresie art. 6, 9 lub 10 RODO stanowią podstawę prawną przetwarzania danych. W razie istnienia podstawy szczegółowej (np. z ustawy prawo bankowe), należy wskazać konkretny przepis i jego związek z przepisami RODO. Należy ocenić zgodność rzeczywistego celu przetwarzania ze wskazaną podstawą prawną przetwarzania
	Opis prawnie uzasadnionych interesów realizowanych przez administratora(w przypadku gdy podstawą przetwarzania jest uzasadniony interes administratora)	

	Kategorie podmiotów, których dane są przetwarzane	Chodzi o rodzaje osób, których dotyczą dane osobowe przetwarzane w ramach procesu. W odniesieniu do istniejących procesów, odpowiedź należy skopiować z opisu czynności przetwarzania. Następnie należy ocenić, czy zakres osób, których dane dotyczą, jest zgodny z celem i podstawą prawną przetwarzania. W razie niezgodności, w rekomendacjach należy wskazać, jaki zakres byłby prawidłowy.
	Kategorie danych osobowych, które są przetwarzane **Kategorie przetwarzanych danych osobowych "zwykłych"** **Kategorie przetwarzanych danych osobowych "szczególnych"**	Chodzi o wszelkie rodzaje przetwarzanych danych osobowych, z wyłączeniem danych wrażliwych (lista poniżej). - Wśród danych osobowych szczególnej kategorii, wymień zakres danych osobowych ujawniających: a) pochodzenie rasowe lub etniczne, b) poglądy polityczne, c) przekonania religijne lub światopoglądowe, d) przynależność do związków zawodowych, e) dane genetyczne, f) dane biometryczne, g) dane dotyczące zdrowia, seksualności lub orientacji seksualnej. - Dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa to odrębna kategoria, o której mowa w art. 10 RODO.
	Czy domyślnie przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania? (art. 25 ust. 2 RODO)	Należy odpowiedzieć, czy co do zasady (domyślnie) przetwarzanie ogranicza się do danych niezbędnych do osiągnięcia celu przetwarzania. Jeżeli nie, należy wskazać niezgodność i wydać odpowiednie rekomendacje. Uwaga: dane niezbędne do osiągnięcia celu przetwarzania, to kategoria węższa, niż dane zgodne z celem przetwarzania. Chodzi o taki zakres danych, bez którego cel przetwarzania nie mógłby zostać osiągnięty.
	Źródło pochodzenia danych **(należy wskazać, czy dane pochodzą od podmiotu danych czy są pozyskiwane z innych źródeł)**	
	Podmioty, którym administrator powierza przetwarzanie danych osobowych / Podstawa prawna powierzenia danych	Chodzi o kategorie osób wewnątrz organizacji, które z upoważnienia administratora mogą przetwarzać dane osobowe. Chodzi o rodzaje podmiotów zewnętrznych, którym powierzono przetwarzanie danych osobowych w imieniu administratora.

	Podmioty, którym administrator udostępnia dane osobowe	Kategorie podmiotów, którym udostępnia się dane osobowe, z wyjątkiem osób wewnątrz organizacji, podmiotów przetwarzających oraz podmiotów publicznych, przetwarzających dane dla potrzeb konkretnego postępowania.
	Podstawa prawna udostępnienia danych przez administratora	
	Odbiorcy danych poza Europejskim Obszarem Gospodarczym/ Podstawa prawna transferu danych poza EOG **Zakres danych osobowych przekazywanych do państwa trzeciego lub organizacji międzynarodowej oraz nazwa tego państwa trzeciego lub organizacji międzynarodowej**	Chodzi o wszelkie rodzaje danych osobowych przekazywanych do państw nienależących do Europejskiego Obszaru Gospodarczego (który obejmuje kraje UE oraz Islandię, Liechtenstein i Norwegię) oraz organizacji międzyrządowych (które powstały na mocy traktatu).
	Współadministratorzy danych **W przypadku współadministrowania – jaki jest podział kompetencji w zakresie przetwarzania danych?**	Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. (art. 26 ust. 1 RODO) Chodzi o ogólny opis, jakie dane przekazywane są pomiędzy którymi podmiotami współadministrującymi danymi i podziału zadań.
	Kto jest właścicielem procesu?	Właściciel procesu to główna osoba odpowiedzialna za jego organizację, projektowanie, zarządzanie zmianami oraz ustawiczne doskonalenie.
	Znaczenie procesu przetwarzania danych dla realizacji zadań PWSZ	
	Funkcjonalny opis operacji przetwarzania	Chodzi o opis występujących w procesie czynności przetwarzania.
	Dane wejściowe w formie elektronicznej	Chodzi o formy lub formaty, w jakich zbierane są dane osobowe w ramach procesu (dane

		cyfrowe).
	Dane wyjściowe - rodzaje dokumentów w formie papierowej	Chodzi o formy, w jakich zbierane są dane osobowe w ramach procesu (dokumenty papierowe).
	Dane wyjściowe - rodzaje dokumentów w formie elektronicznej	Chodzi o formy, w jakich przekazywane są dane osobowe poza proces - w ramach organizacji lub na zewnątrz (dokumenty papierowe).
	Planowane terminy usunięcia poszczególnych kategorii danych lub kryteria ich ustalenia	Dane mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; wyjątkami są, pod pewnymi warunkami, cele archiwalne, interes publiczny, badania naukowe i cele statystyczne.
	Jaki jest stopień poufności danych przetwarzanych w ramach procesu?	Określ poufność danych. Wskazówką może być klasyfikacja danych w ramach ryzyka operacyjnego. Przykładowa skala: a) jawne - dane publicznie dostępne, b) wewnętrzne - dane, do których dostęp mają wyłącznie pracownicy organizacji, c) poufne - dane, do których dostęp mają jedynie ci pracownicy, którym nadano specjalne uprawnienia, d) tajne - dane, których nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla organizacji.
	Ogólny opis fizycznych/ informatycznych technicznych i organizacyjnych środków bezpieczeństwa	Chodzi o ogólny opis, w jaki sposób zabezpieczone są przetwarzane dane osobowe.
	Sprzęt wykorzystywany do przetwarzania danych osobowych **(np. sprzęt komputerowy, sieci)**	

	Systemy informatyczne (oprogramowanie) wykorzystywane do przetwarzania danych osobowych	
	POLITYKI/PROCEDURY WEWNĘTRZNE WDROŻONE PRZEZ ADMINISTRATORA **PRZYJĘTE KODEKSY DOBRYCH PRAKTYK** **PRZYJĘTE CERTYFIKATY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI**	

Analiza ryzyka naruszenia praw i wolności

Ocena ryzyka dokonywana jest na podstawie dwóch kryteriów, kryterium Skutki (wagi) Zagrożenia oraz kryterium Prawdopodobieństwa wystąpienia Zagrożenia:

1) osoba dokonująca oceny powinna- w zakresie każdego wskazanego Zagrożenia - przypisać wartość dla Skutki (1 - 5) oraz Prawdopodobieństwa (1 - 5),
2) wartość dla Skutki należy ustalić biorąc pod uwagę skutki, które może spowodować wystąpienie konkretnego Zagrożenia dla praw i wolności podmiotów danych,
3) wartość dla Prawdopodobieństwa należy ustalić, biorąc pod uwagę możliwość wystąpienia konkretnego Zagrożenia, przy uwzględnieniu środków organizacyjnych, fizycznych oraz technicznych, które zostały wdrożone przez PWSZ lub są objęte planem wdrożenia przed rozpoczęciem Projektu,
4) wartość dla Skutki ustalona dla danego Zagrożenia nie może ulec zmianie w wyniku wdrożenia środków ochrony (jest to wartość stała),
5) wartość dla Prawdopodobieństwa ustalona dla danego Zagrożenia może ulec zmianie w wyniku wdrożenia środków ochrony,
6) stopień potencjalnego ryzyka stanowi iloczyn wartości dla Skutki oraz Prawdopodobieństwa,

Przyjmuje się następujące Stopnie potencjalnego ryzyka:
Niski - gdy iloczyn mieści się w przedziale 1-5,
Średni - gdy iloczyn mieści się w przedziale 6-15,
Wysoki - gdy iloczyn mieści się w przedziale 16-25

KATEGORIE POTENCJALNYCH NARUSZEŃ	ŹRÓDŁA RYZYKA I OPIS POTENCJALNEJ SZKODY	ANALIZA RYZYKA WAGA ZAGROŻENIA, PRAWDOPODOBIEŃSTWO WYSTĄPIENIA I POZIOM RYZYKA	REKOMENDACJE	KONSULTACJA Z ORGANEM NADZORCZYM?
Przetwarzanie nieprawidłowych lub niepełnych danych				
Nieuprawniony dostęp				
Nieuprawnione ujawnienie lub udostępnienie				
Przypadkowe lub nieuprawnione zniszczenie, utrata lub uszkodzenie danych				
Nieuprawniona modyfikacja				
Kradzież tożsamości lub oszustwo dotyczące tożsamości				
Naruszenie zakazu dyskryminacji				
Szkoda finansowa				
Szkoda wizerunkowa				
Złamanie tajemnicy zawodowej				
Wszelkie inne naruszenia praw i wolności osób				

fizycznych				
Całkowity wynik DPIA		[suma wszystkich powyższych pól]	[odpowiedź: wysokie ryzyko / ryzyko]	

VI – OCENA I ZARZĄDZANIE RYZYKIEM

Zagadnienie	
KONSULTACJA Z IOD **sformułowanie zaleceń dotyczących środków minimalizujących ryzyko. W razie potrzeby można zasięgnąć także opinii Działu Administracyjno - Technicznego albo Prawnego.**	
Nazwa dokumentu, do którego przeniesiono rekomendacje wydane w ramach niniejszej DPIA oraz przypisano zadania poszczególnym osobom odpowiedzialnym za utrzymanie zgodności z RODO.	
Ostateczną decyzję o zakresie wdrażanych środków	

VII – KONSULTACJE

Zagadnienie	Odpowiedź
ORGAN NAZDORCZY	
PODMIOTY DANYCH	

VIII – ZASADY MONITOROWANIA I PRZEGLĄDU

Zagadnienie	Odpowiedź
Nazwa dokumentu regulującego zasady monitorowania i przeglądu	
Najbliższy termin weryfikacji konieczności przeprowadzenia DPIA oraz imię i nazwisko osoby odpowiedzialnej	
Najbliższy termin ponownego dokonania DPIA oraz imię i nazwisko osoby odpowiedzialnej	

.....

[data i podpis osoby przeprowadzającej DPIA]

Polityka bezpieczeństwa zawierająca instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy

§ 1.
Postanowienia ogólne

1. Niniejsza Polityka opisuje sposób zabezpieczenia danych osobowych przez Uczelnię oraz sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.
2. Niniejsza Polityka ustanawia zasady ochrony danych osobowych przy:
a) zarządzaniu ruchem sieciowym i bezpieczeństwem komunikacji,
b) zapewnianiu bezpieczeństwa fizycznego i środowiskowego informacji,
c) zapewnianiu ciągłości działania organizacji, w tym poprzez stosowanie kopii zapasowych,
d) ochronie przed szkodliwym oprogramowaniem,
e) zapewnieniu bezpieczeństwa urządzeń mobilnych i telepracy,
f) klasyfikacji informacji i kontroli dostępu,
g) zabezpieczeniach kryptograficznych i pseudonimizacji.
3. Uczelnia zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Uczelnię. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
4. Wszelkie wnioski i zgłoszenia napraw, awarii należy zgłaszać przez pocztę email do pracowników Sekcji inwentaryzacji.
5. Za bezpieczeństwo:
a) fizyczne i techniczne przetwarzania danych osobowych odpowiedzialni są kierownicy komórek organizacyjnych Uczelni.
b) za bezpieczeństwo związane z przetwarzaniem danych osobowych za pomocą sieci, systemów i urządzeń IT odpowiedzialny jest Główny informatyk.
6. IOD sprawuje nadzór nad realizacją zadań mających na celu osiągnięcie zgodności z zasadą, o której mowa w art. 5 ust. 1 lit. f RODO oraz nad wdrożeniem środków, o których mowa w ust. 32 ust. 1 RODO.

§ 2.
Analiza ryzyka

1. Administrator:
1) dokonuje identyfikacji zasobów danych osobowych, klasyfikacji przetwarzanych danych, zależności między zasobami danych osobowych, identyfikacji sposobów wykorzystania danych (inwentaryzacja),
2) prowadzi rejestr aktywów służących przetwarzaniu danych osobowych,
3) ustala i monitoruje zagrożenia dla aktywów służących przetwarzaniu danych osobowych.
4) ustala i monitoruje zabezpieczenia służące bezpieczeństwu danych osobowych
5) dokonuje analizy ryzyka w oparciu o metodykę przyjętą w Załączniku nr 3 do Polityki Ochrony Danych Osobowych.

§ 3.
Zabezpieczenia

1. Administrator ustala możliwe do zastosowania na Uczelni zabezpieczenia danych osobowych w zakresie zabezpieczeń organizacyjnych, technicznych i fizycznych niezbędne dla zapewnienia poufności, integralności, dostępności, rozliczalności i ciągłości przetwarzanych danych i ocenia koszt ich wdrażania.
2. W celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w ramach ruchu sieciowego oraz komunikacji elektronicznej, sieć oraz połączenia należy chronić przy pomocy:
a) zapory sieciowej,
b) monitorowania i automatycznego rejestrowania zdarzeń ruchu sieciowego,
c) każdorazowej identyfikacji i uwierzytelnianiu użytkowników połączonych z siecią,
d) kontroli dostępu użytkowników,
e) wdrożenia zasad ciągłości działania, zgodnie z Procedurą przywrócenia dostępności danych osobowych,
f) wdrożenia ochrony przed szkodliwym oprogramowaniem,
g) ograniczenia połączeń systemów do sieci.
4. Uczelnia tam gdzie jest to możliwe i uzasadnione stosuje:
a) Pseudonimizację – w każdej sytuacji przesyłu danych osobowych w ramach rożnych procesów biznesowych należy rozważyć możliwość dokonania pseudonimizacji,
b) szyfrowanie danych osobowych,
c) środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania takie jak: antywirusy, firewalle, oprogramowania do zarządzania dostępami do zasobów, systemów,
d) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego takie jak: kopie zapasowe baz danych, kopie licencji,
e) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

f) wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów,
g) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe,
h) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall,
i) Ochronę sprzętu komputerowego przed złośliwym oprogramowaniem,
j) Zabezpieczenie dostępu do urządzeń przy pomocy haseł dostępu,
k) Wykorzystanie szyfrowania danych przy ich transmisji.
5. Zasoby uczestniczące w operacjach przetwarzania danych osobowych należy użytkować i przechowywać w lokalizacjach odpowiednio zabezpieczonych przed zagrożeniami fizycznymi i środowiskowymi. Lokalizacje są odpowiednio zabezpieczone przed zagrożeniami fizycznymi i środowiskowymi, jeżeli:
a) nie występują luki w granicach budynku,
b) nie występują wady konstrukcyjne budynku,
c) budynek jest wyposażony w instalację odgromową, przeciwpożarową,
d) budynek oraz drzwi wejściowe są chronione systemem alarmowym,
e) dostęp do pomieszczeń jest ograniczony do jednej organizacji i wymaga posiadania klucza lub karty dostępu,
f) okna narażone na dostęp osób trzecich mają dodatkowe zabezpieczenia (np. kraty, szyby antywłamaniowe),
g) drzwi wejściowe i okna narażone na dostęp posiadają systemy wykrywania włamań,
h) przewody zasilające i komunikacyjne są chronione przed przepięciami.
6. Dostęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania danych osobowych, należy w miarę możliwości ograniczyć do osób upoważnionych do przetwarzania danych osobowych przy wykorzystaniu tych zasobów.
7. W celu zapewnienia integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych, stosuje się zasady ciągłości działania. Zasady ciągłości działania obejmują obowiązek:
a) objęcia wszystkich urządzeń sieciowych i stacji roboczych przetwarzających dane osobowe zasilaniem awaryjnym UPSy,
b) przechowywania danych osobowych w wersji elektronicznej na służbowym dysku sieciowym,
c) tworzenia kopii zapasowych danych znajdujących się na stacjach roboczych, urządzeniach mobilnych oraz na służbowym dysku sieciowym,
d) szyfrowania kopii zapasowych i przechowywania ich w bezpiecznym miejscu, z dala od źródeł zagrożeń dla zasobów, z których kopie zapasowe są wykonywane,
e) regularnego testowania możliwości szybkiego przywrócenia dostępności danych osobowych odzyskanych z kopii zapasowych,
f) prowadzenia listy kopii zapasowych,
g) zabezpieczenia przewodów służących do zasilania lub przekazywania informacji,
h) wyznaczenia osób odpowiedzialnych za obsługę zgłoszeń incydentów i jak najszybsze przywrócenie dostępności.
8. W celu zapewnienia rozliczalności, zegary systemów informatycznych objętych rejestracją zdarzeń powinny być zsynchronizowane z tym samym serwerem czasu.
9. Określając zakres i częstotliwość wykonywania kopii zapasowych, należy wziąć pod uwagę wyniki analizy ryzyka dla zasobów uczestniczących w operacjach przetwarzania danych osobowych.
10. Dostęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania danych osobowych, należy ograniczyć do:
a) osób uprawnionych do przetwarzania danych osobowych przy wykorzystaniu tych zasobów, którym przyznano odpowiedni klucz lub kartę dostępu,
b) personelu technicznego i sprzątającego – o ile ich dostęp następuje pod nadzorem osób upoważnionych do przetwarzania danych osobowych lub jest w inny sposób monitorowany, a przetwarzane w pomieszczeniach dane osobowe są odpowiednio zabezpieczone przed dostępem,
c) gości organizacji – o ile ich tożsamość jest weryfikowana, daty i godziny wejść i wyjść są rejestrowane, a dostęp następuje pod nadzorem osób upoważnionych do przetwarzania danych osobowych.

§ 4.
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.

1. Dane osobowe przetwarzane są w PWSZ im. Witelona w Legnicy z użyciem dedykowanych serwerów oraz komputerów stacjonarnych.
2. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, ASI (Administrator Systemów Informatycznych) ustala niepowtarzalny login.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym możliwy jest wyłącznie po podaniu przez użytkownika loginu i właściwego hasła dostępu.
4. Główny informatyk lub osoba przez niego upoważniona tj. ASI przekazując użytkownikowi login i hasło przeprowadza szkolenie z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.
5. Za realizację procedury rejestrowania, aktualizacji oraz wyrejestrowywania użytkowników w systemie informatycznym odpowiedzialny jest ASI.
6. Użytkownicy nie mogą korzystać z innych loginów niż ten, który został im nadany.
7. Login użytkownika nie podlega zmianie, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie jest przydzielany innej osobie.
8. Główny informatyk wyznacza dla każdego systemu informatycznego ASI oraz osobę zastępującą, w przypadku jego nieobecności. ASI przydziela się w systemie login użytkownika uprzywilejowanego.

9. Kierownik komórki organizacyjnej, informuje głównego informatyka o fakcie utraty przez podległą mu osobę uprawnień dostępu do danych osobowych w systemie informatycznym.
10. Login osoby, która utraciła uprawnienia dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 5.
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Hasło ustanowione podczas przyznawania uprawnień przez ASI należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
2. Hasło dostępu użytkownika ulega automatycznej zmianie raz na miesiąc. Za jego zmianę odpowiedzialny jest użytkownik.
3. Hasło składa się z co najmniej ośmiu znaków, zawiera małe i duże litery oraz cyfry lub znaki specjalne.
4. Hasło nie może być udostępniane innym użytkownikom ani przechowywane w miejscach umożliwiających dostęp do niego osobom trzecim.
5. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie ASI.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego loginu i hasła dostępu.
8. Stanowiska komputerowe, na których skonfigurowanie loginu i hasła zapewniającego ochronę jest nieskuteczne, zabezpiecza się dodatkowym hasłem (hasło wygaszacza ekranu, hasło BIOSu)
9. Hasła ASI są zdeponowane w Kancelarii Tajnej i podlegają zmianie raz w roku.
10. W stosunku do haseł użytkowników uprzywilejowanych stosuje się zaostrzone standardy bezpieczeństwa. Standardy, te stosuje się również do haseł:
1) elementów aktywnych sieci teleinformatycznych;
2) konfiguracji komputerów, w tym hasła do BIOS.
11. Hasła przechowuje się w postaci zaszyfrowanej.
12. Do przechowywania haseł zapisanych na papierze stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne").
13. Koperty z hasłami przechowuje się w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym albo w zaszyfrowanym pliku w odrębnej lokalizacji.
14. Dane umieszczone na bezpiecznej kopercie zawierają:
a) numer koperty adekwatny do numeru ewidencyjnego podanego w ewidencji haseł;
b) datę jej złożenia i podpis osoby składającej kopertę;
15. Koperty z hasłami podlegają ścisłej ewidencji prowadzonej przez ASI.
16. Ewidencja haseł przechowywana jest w miejscu zabezpieczonym przed dostępem osób niepowołanych.
17. Za aktualność przechowywanych haseł odpowiedzialny jest ASI.
18. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga udokumentowane w ewidencji kopert. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.
19. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
20. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez ASI) i jego przechowywanie.
21. Każdy użytkownik posiadający dostęp do systemu informatycznego jest obowiązany do:
1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;
4) poinformowania ASI o podejrzeniu lub rzeczywistym ujawnieniu hasła;
5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
6) stosowania haseł nie posiadających w swojej strukturze części login;
7) Stosowania haseł nie będących zbliżonymi do poprzednich (np. Tadeusz$2013 - Tadeusz$2014);
8) Zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.

22. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
23. Zabronione jest:
a) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
b) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
c) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
d) udostępnianie haseł innym użytkownikom;
e) przeprowadzanie prób łamania haseł;
f) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).
24. ASI obowiązany jest do skonfigurowania systemu, aby próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym, jak i czasowym jeżeli system umożliwia wymienioną konfigurację.

25. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 3, po czym ustanowić blokadę konta.
26. ASI ogranicza możliwość wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator.
27. ASI odblokowuje/zresetuje hasło do danego systemu informatycznego w przypadku przekroczenia przez użytkownika ustalonej ilości prób logowania. Po dokonaniu czynności przez ASI stosowną informacja o odblokowaniu dostępu do konta użytkownika zostanie przekazana użytkownikowi.

§ 6.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Dane osobowe, których Administratorem jest PWSZ im. Witelona w Legnicy mogą być przetwarzane z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych Uczelni.
2. Użytkownik przystępujący do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe wpisuje login oraz hasło dostępu, a po uzyskaniu akceptacji uruchamia właściwy program.
3. Użytkownik ma obowiązek wylogowania się lub zablokowania systemu w przypadku nieobecności na stanowisku pracy lub w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim użytkownika.
4. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.
5. Po zakończeniu pracy należy zamknąć programy i po zastosowaniu odpowiedniej procedury wyłączyć komputer.
6. Wychodząc z pomieszczenia, w którym przetwarzane są dane z systemu informatycznego należy sprawdzić czy zamknięte są okna i wejście do pomieszczenia.
7. Użytkownik niezwłocznie powiadamia ASI o przypadku braku możliwości zalogowania się na swoje konto oraz Kierownika swojej komórki organizacyjnej w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.
8. Drukarki nie mogą być pozostawione bez kontroli jeśli są lub wkrótce będą drukowane na nich dane osobowe z systemu informatycznego, o ile dostęp osób trzecich do pomieszczeń drukarek nie jest odpowiednio ograniczony.
9. Drukowanie na takich drukarkach jest dopuszczalne o ile otoczenie drukarki jest chronione przed fizycznym dostępem osób nieuprawnionych.
10. Za przechowywanie wydruku zawierającego dane z systemu informatycznego w PWSZ im. Witelona w Legnicy odpowiada użytkownik tj. wykonawca wydruku.
11. Wykonawca który odpowiada za przechowywanie wydruku zawierającego dane z systemu informatycznego, może przekazać wydruk oraz odpowiedzialność za jego przechowanie innej osobie tylko wtedy, gdy jest ona upoważniona do dostępu informacji zawartych na wydruku.
12. Wydruki zawierające dane z systemu informatycznego po zakończeniu pracy powinny być przechowywane w zamkniętych szafach.
13. Wydruki, notatki, kserokopie dokumentów itp. nie wykorzystane a zawierające dane osobowe z systemu informatycznego muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.

§ 7.
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Kopie zapasowe systemów, aplikacji baz danych i dokumentów użytkowanych przez Uczelnię służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji systemów i aplikacji.
2. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
b) sporządzania kopii zapasowych zbiorów danych (kopie pełne).
3. Główny informatyk odpowiedzialny jest za tworzenie kopii bezpieczeństwa systemu informatycznego, przy czym może on zlecić wykonanie tej kopii wyznaczonemu ASI.
4. Pełne kopie zapasowe zbiorów danych tworzone są codziennie po zakończonym dniu pracy.
5. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.
6. Po utworzeniu kopii automatycznie (jeżeli jest technicznie realizowalne) jest generowany raport o przebiegu wykonania kopii. Raport podlega weryfikacji przez administratora systemu informatycznego.
7. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia gdyby doszło do awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest właściwy ASI.
8. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
9. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością PWSZ im. Witelona w Legnicy, użytkownik systemu ma obowiązek sporządzania kopii zapasowych jak również ochrony nośników informacji. Wymaga się od użytkownika stosowania zasad dotyczących ochrony danych osobowych przed dostępem osób nieuprawnionych.

10. Regularnie, co najmniej raz w roku, ASI przeprowadza testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu, jeżeli jest prowadzony.
11. W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych lub biznesowych, dane z nośników są przenoszone na inny nośnik.
12. Nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi w niniejszej Polityce.
13. Po upływie wymaganego okresu przechowywania kopie archiwalne są niszczone zgodnie z zasadami określonymi w niniejszej Polityce.
14. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub archiwalnych.
15. Kopie bezpieczeństwa są wykonywane:
1) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
2) przed dokonaniem zmian w programach (np. zmiana wersji);
3) przed i/lub po każdej istotnej zmianie danych w bazie danych;
16. Oprócz kopii, o których mowa w ust. 15 są wykonywane kopie archiwalne:
1) miesięczne – na koniec danego miesiąca;
2) roczne – na koniec danego roku;
17. Pliki użytkowników systemu informatycznego są przechowywane na indywidualnie udostępnionych dyskach serwerów.
18. Dyski serwerów zabezpiecza się przed utratą danych w postaci kopii bezpieczeństwa i/lub archiwalnych.
19.Kopie bezpieczeństwa oraz kopie archiwalne są:
a) wykonywane w co najmniej jednym egzemplarzu;
b) przechowywane w innym miejscu niż te, w którym zbiory eksploatowane są na bieżąco (co najmniej w innej strefie pożarowej).
c) w trakcie transportu zabezpieczane przed osobami nieupoważnionymi i niekorzystnymi zjawiskami fizycznymi mogącymi doprowadzić do ich zniszczenia bądź uszkodzenia;
20. Kopie bezpieczeństwa są przechowywane do momentu wykonania następnej kopii bezpieczeństwa. Kopie bezpieczeństwa usuwa się po sporządzeniu kolejnej kopii.

§ 8.
Sposób, miejsce i okres przechowywania nośników informacji zawierających dane osobowe, w tym kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na płytach CD, DVD, kasetach do streamerów lub innych elektronicznych nośnikach informacji. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.
2. Kopie są przechowywane w bezpiecznej odległości (co najmniej w innej strefie pożarowej) od miejsca, w którym jest prowadzona eksploatacja systemów.
3. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Rektor, Kanclerz, Główny Informatyk, IOD oraz ASI.
4. Kopie miesięczne przechowuje się przez okres 6 miesięcy. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
5. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
6. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika, za ich zniszczenie odpowiada użytkownik.
7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
8. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
9. W przypadku braku możliwości zrealizowania procedury zniszczenia nośników informacji, należy fakt ten zgłosić głównemu informatykowi. Po przekazaniu nośników zostaną one zniszczone w ramach środków technicznych Działu Administracyjno-Technicznego, bądź poddane procedurze utylizacji nośników informacji realizowanej przez firmę zewnętrzną.
10. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy należy pozbawić przed naprawą zapisu danych albo naprawiać pod nadzorem osoby upoważnionej przez ADO.

§ 9.
Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. Ruch w sieci komputerowej PWSZ im. Witelona w Legnicy jest zabezpieczony przed dostępem z zewnętrznej publicznej sieci przez zastosowanie rozbudowanej ściany ogniowej (firewall).

2. Na wszystkich stacjach roboczych oraz serwerach zainstalowane jest oprogramowanie antywirusowe Eset Endpoint Antivirus.
3. Aktualizacje baz danych pobierane są codziennie do lokalnego repozytorium, z którego aktualizacje pobierane są przez pozostałe komputery.
4. Funkcjonowanie oprogramowania antywirusowego nadzorowane jest centralnie przez oprogramowanie konsoli zarządzającej.
5. Użytkownicy powinni być przeszkoleni w ramach wewnętrznych szkoleń adaptacyjnych, w szczególności z zasad bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania oraz zasad postępowania w przypadku wykrycia, lub podejrzenia działania złośliwego oprogramowania.
6. Oprogramowanie używane w systemie informatycznym w PWSZ im. Witelona w Legnicy musi być chronione przed jakąkolwiek niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz kopiowaniem.
7. Przed jakimkolwiek zainstalowaniem nowego oprogramowania należy sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
8. W systemie informatycznym w PWSZ im. Witelona w Legnicy może być używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich.
9. Oprogramowanie może być używane tylko zgodnie z prawami licencji.
10. Narzędzia związane z bezpieczeństwem systemów mogą być wykorzystane w systemie informatycznym w PWSZ im. Witelona w Legnicy tylko jeśli pochodzą od zaufanego dostawcy.
11. ASI raz w miesiącu dokonuje sprawdzenia serwera przy użyciu uaktualnionego oprogramowania antywirusowego.
12. Użytkownik przeprowadza cykliczne kontrole antywirusowe w przydzielonym mu komputerze - minimum raz w miesiącu. W przypadku wykrycia wirusów komputerowych, sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki
13. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze, w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowaniu.
14. W przypadku podejrzenia wykrycia wirusa komputerowego użytkownik powinien natychmiast powiadomić o tym głównego informatyka lub ASI.
15. Bez zgody głównego informatyka oraz ASI zabronione jest instalowanie jakiegokolwiek oprogramowania komputerowego.
16. Pobieranie w niezbędnym zakresie danych ze źródeł zewnętrznych możliwe jest wyłącznie po uprzednim ich sprawdzeniu na obecność wirusów komputerowych.
17. Autoryzowane, do używania z systemu informatycznego w PWSZ im. Witelona w Legnicy, nośniki informacji powinny być po zakończeniu pracy przechowywane w sposób zapewniający bezpieczeństwo zapisanych na nim danych.
18. W przypadku uszkodzenia lub zużycia płyty CD-ROM lub inne komputerowe nośniki winny być zdawane głównemu informatykowi.
19. Główny informatyk dokonuje zniszczenia uszkodzonego lub zużytego komputerowego nośnika informacji w sposób uniemożliwiający odtworzenie zapisanych na nim danych.

§ 10.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje na bieżąco wyznaczony przez głównego informatyka ASI – nie rzadziej niż raz w miesiącu. Sprawdzana jest spójność danych, indeksów oraz stan nośników informacji, np. dysków twardych oraz urządzeń peryferyjnych.
2. Za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty e-mail, a także za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
3. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych nadzorowane są przez IOD i wykonywane są przez administratorów właściwych systemów informatycznych w pomieszczeniach stanowiących obszar przetwarzania danych.
4. Przeglądy techniczne i konserwacja systemu powinny być wykonywane w terminach określonych przez producentów lub zgodnie z harmonogramem ASI, jednak nie rzadziej niż raz w roku, a także w trakcie przygotowania do dużych aktualizacji systemów.
5. Przeglądy i konserwacje w zależności od systemu, powinny zawierać czynności związane z:
1) analizą zdarzeń i logów systemowych w celu wykrycia niestandardowych zachowań,
2) kontrolą zajętości dysku twardego oraz usuwanie zbędnych danych (np. bardzo stare logi zdarzeń, pliki tymczasowe „temp", tymczasowe kopie zbiorów danych, itp.)
3) kontrolą obciążenia procesora i uruchomionych procesów w systemie operacyjnym,
4) kontrolą poprawności funkcjonowania zabezpieczeń przed nieuprawnionym dostępem do zbiorów.
6. ASI okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest ustalana przez głównego informatyka.
7. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa została sprawdzona na rynku – z pełnym zastosowaniem procedur obowiązujących w PWSZ im. Witelona w Legnicy.
8. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz wyznaczonego przez głównego informatyka pracownika, w miejscu jego użytkowania.
9. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.

10. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą głównego informatyka.
11. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością PWSZ im. Witelona w Legnicy użytkownik systemu jest odpowiedzialny za zabezpieczenie danych osobowych znajdujących się na jego komputerze, przed przekazaniem sprzętu do serwisu.
12. W przypadku problemów z realizacją zabezpieczenia danych osobowych, użytkownik systemu zobowiązany jest zwrócić się o pomoc, w tym zakresie, do pracowników Sekcji informatyki.
13. Niesprawne nośniki danych, na których przechowywano dane osobowe powinny być niszczone trwale, aby nie był możliwy odczyt z nich jakichkolwiek danych.
14. Uszkodzone urządzenia i nośniki, które zawierają dane osobowe, powinny być trwale niszczone fizycznie. W przypadku braku możliwości zakupu nowych urządzeń lub nośników oraz odtworzenia utraconych danych z kopii zapasowych, należy podjąć ich naprawę na miejscu w obecności upoważnionego pracownika.
15. W przypadku zbywania/darowizny komputerów lub nośników wykorzystywanych dotychczas przez PWSZ im. Witelona w Legnicy wszystkie dane osobowe w nich zawarte powinny być wykasowywane nieodwracalnie.
16. Uszkodzone urządzenie lub nośnik nie będący własnością PWSZ im. Witelona w Legnicy, na którym znajdują się dane osobowe powinien być trwale niszczony fizycznie lub naprawiany w obecności użytkownika.
17. Osobą odpowiedzialną za okresową weryfikację uprawnień poszczególnych użytkowników aplikacji jest główny informatyk.
18. Poszczególne systemy informatyczne muszą w sposób bezpieczny prowadzić zapis wszystkich znaczących zdarzeń systemowych mających wpływ na bezpieczeństwo przetwarzanych w nich danych osobowych a w szczególności:
a) zmian loginu użytkownika w czasie sesji,
b) prób odgadywania haseł,
c) prób wykorzystania uprawnień, do których użytkownik nie uzyskał autoryzacji,
d) modyfikacji oprogramowania aplikacyjnego,
e) modyfikacji oprogramowania systemowego,
f) zmian uprawnień użytkowników,
g) prób ingerencji w systemowe rejestry zdarzeń.
19. Rejestry zdarzeń systemowych związanych z bezpieczeństwem systemów informatycznych muszą być przechowywane przez okres co najmniej jednego miesiąca.
20. Podczas tego okresu muszą być zabezpieczone w taki sposób aby nie była możliwa ich modyfikacja oraz aby były one dostępne jedynie dla autoryzowanych pracowników.
21. ASI powinien codziennie kontrolować zbiory systemowe dla prawidłowego funkcjonowania systemu.
22. Główny informatyk co najmniej raz na kwartał winien przeprowadzić weryfikację usług sieciowych dostępnych w systemach informatycznych oraz blokować usługi niewykorzystywane.
23. Główny informatyk jest odpowiedzialny za uaktualnianie systemów operacyjnych i aplikacji.
24. Osoba wyznaczona wraz z głównym informatykiem raz na miesiąc, a w przypadku podejrzeń naruszenia zabezpieczeń danych osobowych z uwagi na stan urządzeń lub sposób działania programu, bezzwłocznie:
a) sprawdzają serwer oraz poszczególne komputery za pomocą istniejących w systemie informatycznym programów monitorujących,
b) dokonują przeglądu i bieżącej konserwacji sprzętu oraz zbioru danych.

§ 12.
Pseudonimizacja i kryptografia

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji wewnętrznych Uczelni powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada ASI.
3 Przekazywanie kluczy użytkownikom odbywa się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
4. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
5. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić ASI.
6. Dane osobowe wrażliwe lub informacje wewnętrzne Administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
7. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
8. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić ASI.
9. Przy sprzętach mobilnych można używać szyfrowania wbudowanego w urządzenie.
10. W przypadku przesyłania danych osobowych poza Uczelnię należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy innym kanałem komunikacji np. telefonicznie lub SMS.

§ 13.
Bezpieczne korzystanie ze sprzętu IT w którym przetwarzane są dane osobowe

1. Do sprzętu komputerowego zalicza się między innymi:
a) komputery stacjonarne;
b) komputery przenośne;
c) tablety;

d) smartphony;
e) drukarki;
f) modemy;
g) monitory;
h) routery;
i) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. ASI odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą ASI może wykonywać poprzez pracowników lub współpracowników ASI lub poprzez podmioty zewnętrzne.
3. W przypadku wykorzystywania urządzeń mobilnych (m.in. tablet, smartphone) wymaga się zastosowania następujących środków bezpieczeństwa:
a) blokada ekranu (pin/hasło/symbol graficzny);
b) szyfrowanie pamięci/karty pamięci;
c) program antywirusowy;
d) wyłączanie nieużywanych usług (wi-fi, gprs/lte, bluetooth, nfc);
e) instalowanie oprogramowania z zaufanego źródła (np. iStore, Google Play);
f) używanie szyfrowania, np.: poczty lub VPN podczas korzystania z publicznych hotspot–ów.
4. Przekazanie sprzętu jest to czynność polegająca na dostarczeniu sprzętu komputowego wraz z odpowiednim oprogramowaniem użytkownikowi.
5. ASI odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.
6. ASI jest zobowiązany do prowadzenia spisu posiadanego pod opieką sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją.
7. ASI ma obowiązek przechowywać karty gwarancyjne, klucze i licencje do oprogramowania.
9. ASI prowadzi rejestr wydanego sprzętu komputerowego wraz z wyszczególnieniem użytkownika. ASI udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
10. ASI ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
11. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
12. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.
13. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.
14. W celu zapewnienia bezpieczeństwa danych osobowych przy korzystaniu z urządzeń mobilnych i telepracy, ASI lub osoba przez niego upoważniona przed dopuszczeniem do użytku konfiguruje urządzenie mobilne:
a) zakładając profil użytkownika, ochronę hasłem i blokadę ekranu zgodnie z zasadami kontroli dostępu,
b) szyfrując dane zgodnie z zasadami zabezpieczeń kryptograficznych,
c) instalując ochronę przed szkodliwym oprogramowaniem,
d) konfigurując tunel wirtualnej sieci prywatnej (VPN) i dostęp do służbowego dysku sieciowego,
e) ograniczając możliwość instalowania i odinstalowywania oprogramowania,
f) konfigurując możliwość zdalnego zablokowania urządzenia w przypadku kradzieży.
15. ASI lub osoba przez niego upoważniona, prowadzi rejestr urządzeń mobilnych.
16. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany danych osobowych lub informacji poufnych Uczelni, jeśli rozmowy te odbywają się w miejscach publicznych, pomieszczeniach które nie gwarantują zachowania poufności rozmów.
17. Przekazywanie dokumentów zawierających dane osobowe szczególnej kategorii bez ich zabezpieczenia (np. zaszyfrowania) jest zabronione.

§ 14.
Procedura niszczenia nośników zawierających dane osobowe

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a w szczególności:
a) twarde dyski z danymi osobowymi ze stacji roboczych i laptopów
b) pendrive
c) pamięci flash
d) dyski SSD
e) płyty DVD
f) telefony komórkowe / smartfony
są niszczone w sposób fizyczny w tym również komisyjnie. Z procesu niszczenia sporządza się Protokół zniszczenia uszkodzonych nośników.
2. Stosowane metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera / zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.
3. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów)

4. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie albo za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji).

§ 15.
Zabezpieczenia fizycznego dostępu i Polityka kluczy

1. Budynki Uczelni są objęte monitoringiem wizyjnym, systemem alarmowym.
2. Budynek przy ul. Sejmowej 5A, 5C oraz Mickiewicza 10 podlega dozorowi i ochronie polegającej na:
a) całodobowym monitorowaniu przez firmę zewnętrzną lokalnego systemu alarmowego zamontowanego w obiekcie,
b) całodobowym monitoringu wizualnym za pomocą lokalnego systemu kamer oraz rejestratora video zamontowanego w obiekcie.
c) ochronie dostępu do pomieszczeń poprzez zapewnienie kontroli dostępu przez ochronę na portierni.
3. Konserwację i naprawę systemu alarmowego i monitoringu wizualnego w sposób zapewniający bezawaryjne jego działanie wykonuje zewnętrzna firma.
4. W godzinach pracy Uczelni zobowiązuje się pracowników w szczególności do:
a) zwracania uwagi na zachowanie osób wchodzących i wychodzących,
b) reagowania na wejście do budynku i przebywanie w strefie administracyjnej osób będących pod wpływem alkoholu lub podobnie działającego środka,
c) reagowania na próby niszczenia lub wynoszenia mienia z obiektu Uczelni,
d) reagowania na próby wnoszenia do obiektu Urzędu przedmiotów i materiałów niebezpiecznych,
e) natychmiastowego reagowania poprzez powiadomienie odpowiednich służb oraz osób o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.
5. Wszystkie klucze od pomieszczeń Uczelni znajdują się pod nadzorem ochrony w szafie przy portierni.
6. Kopie kluczy znajdują się w odrębnej szafce zamykanej na klucz w pomieszczeniu wyznaczonym przez Administratora.
7. Pracownik odpowiedzialny za nadzór nad szafami zamykanymi na klucz, w których są przechowywane dokumenty zawierające dane osobowe zobowiązany jest po zakończeniu pracy zamknąć klucze w jednej szafce lub szufladzie zamykanej na klucz.
8. Pracownik, który pobrał klucz(e) od pomieszczenia(eń), przed uruchomieniem zamków sprawdza od strony wizualnej stan tych zamków i ewentualnych zabezpieczeń zastosowanych przy zamykaniu pomieszczeń, a także używanych plomb (jeżeli takie są przewidziane).
9. Po otwarciu pomieszczeń biurowych, jeszcze przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tych pomieszczeniach dokumentacji i innego wyposażenia.
10. W przypadku stwierdzenia zmian lub naruszeń stanu zabezpieczeń pracownik, który to stwierdził, natychmiast powiadamia o tym fakcie bezpośrednio przełożonego.
11. Od momentu pobrania kluczy do momentu ich zdania na pracownikach spoczywa odpowiedzialność za ochronę kluczy i pomieszczeń biurowych.
12. W przypadku utraty, uszkodzenia lub zniszczenia kluczy użytkownik niezwłocznie powiadamia o tym fakcie bezpośrednio przełożonego.
13. Po zakończeniu dnia pracy, pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających, adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających głównie na:
a) zabezpieczeniu dokumentacji,
b) zabezpieczeniu komputerów,
c) wyłączeniu urządzeń energetycznych zasilanych energią elektryczną,
d) zamknięciu okien i drzwi,
e) zdaniu kluczy od pomieszczeń.
14. Klucze od biurek stanowiskowych, szaf biurowych i pieczątek są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
15. Po godzinach pracy biurka, szafy zawierające klucze i pieczątki są zamykane.
16. Wydawanie kluczy zapasowych pracownikom uprawnionym do ich pobrania może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych przez Administratora budynku. Na powyższą okoliczność sporządza się notatkę służbową. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu. Dorabianie kluczy do pomieszczeń i budynku wymaga zgody Kierownika Działu Administracyjno - Technicznego i dozwolone jest wyłącznie w celu zastąpienia kluczy utraconych, uszkodzonych lub zniszczonych.
17. Jeżeli z okoliczności udostępnienia kluczy osobie nieupoważnionej lub jego utraty wynika, że może zostać wykorzystany do nieuprawnionego dostępu do pomieszczeń lub budynku, należy wymienić odpowiedni zamek lub jego elementy. O zaistniałej sytuacji należy niezwłocznie powiadomić bezpośrednio przełożonego.
18. Zabrania się:
a) udostępniania kluczy osobom nieupoważnionym,
b) pozostawiania otwartych pomieszczeń lub kluczy bez dozoru,
c) pozostawiania otwartych okien po zakończeniu pracy.

§ 16.
Polityka drukowania, czystego biurka

1. Wszystkich pracowników Uczelni obowiązuje:
a) Zasada czystego biurka – należy unikać pozostawiania dokumentów zawierających dane osobowe na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych, płyt CD lub innych nośników danych; Na

stanowiskach pracy należy dbać, by po zakończeniu pracy wszystkie dokumenty zawierające dane osobowe były chowane do szaf zamykanych na klucz.

b) Zasada czystego ekranu – każdy komputer musi mieć ustawiony wygaszacz ekranu. Wygaszacz powinien włączać się automatycznie po minimum 15 minutach bezczynności użytkownika. Użytkownicy powinni przed pozostawieniem włączonego komputera bez opieki, zablokować komputer lub w przypadku dłuższej nieobecności wylogować się z systemu. Po zakończonym dniu komputer powinien zostać wyłączony;

c) Zasada czystych drukarek – informacje zawierające dane osobowe powinny być zabierane z drukarek natychmiast po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za dane urządzenie lub zgłosić incydent bezpieczeństwa; Pracownik, który ustali nieznanego pochodzenia wydruk znajdujący się w drukarce, po uprzedniej próbie ustalenia, do kogo należy wydruk zobowiązany jest do zniszczenia w niszczarce pozostawionego dokumentu.

d) Zasada czystego kosza – dokumenty papierowe zawierające dane osobowe powinny być niszczone w sposób uniemożliwiający ich odczytanie (w niszczarce).

FORMULARZ OCENY NOWEGO PROJEKTU (PRIVACY BY DESIGN)

LP.	PYTANIE	WYJAŚNIENIA	KOMENTARZ OSOBY WYPEŁNIAJĄCEJ
1.	**Proszę opisać na czym ma polegać nowy projekt w którym będą przetwarzane dane osobowe**	Czego dotyczy Projekt? Opisz krótko. W opisie należy uwzględnić: - jakie dane będą pozyskiwane i przez jaki kanał, - jacy pracownicy będą dane pobierać lub jaki ma być schemat przepływu danych od momentu wpłynięcia do usunięcia - założenia dotyczące tego, kto i na jakich zasadach ma uzyskiwać dostępu do danych osobowych gromadzonych w związku z realizacją Projektu np.: 1. w przypadku nowego typu konkursu - w jaki sposób będzie publikowana lista /uczestników laureatów (czy ich dane będą dostępne w Internecie lub wywieszane w miejscu dostępnym dla osób nie zatrudnionych w organizacji) 2. w przypadku stworzenia gazetki zawierającej informacje o PWSZ (np. prywatne zdjęcia, wspomnienia z wakacji KÓŁ NAUKOWYCH gdzie będzie dystrybuowana i dostępna, czy dostęp do niej mogą uzyskiwać osoby spoza PWSZ, czy potrzebne będą zgody na wizerunek itp. 3. nowy system IT albo nowa funkcjonalność w koncie użytkownika systemu IT obsługiwanego przez PWSZ – czy i jak będą dane pobierane, na czym polega funkcjonalność i jak ma wykorzystywać dane osobowe	
2.	**Proszę opisać Cele Projektu**	Jakie są cele Projektu? Opisz krótko, czemu będziesz przetwarzać dane w tym Projekcie. Uwzględnij nie tylko cel główny ale także cele poboczne *(np. zbieranie leadów w celu ew. późniejszego kontaktu marketingowego)* Przykładowe cele to: 1. promocja PWSZ nowy konkurs 2. konferencja międzynarodowa 3. wykrywanie nadużyć, bezpieczeństwo sieci 4. marketing własnych usług edukacyjnych/szkoleniowych 5. marketing cudzych usług 6. rekrutacja z użyciem nowego oprogramowania HR 7. wykonanie umowy z pracownikiem 8. poprawa jakości świadczonych usług 9. cele analityczne i statystyczne 10. obsługa studenta 11. realizacja obowiązków publicznoprawnych 12. dochodzenie roszczeń	
3.	**Proszę opisać kategorie osób, których dane**	Odpowiadając na to pytanie wskaż, czyje dane osobowe przetwarzasz.	

	mają być wykorzystane w Projekcie	**Przykładowe** kategorie osób, których dane dotyczą: 1. studenci 2. uczestnicy konkursu 3. uczestnicy konferencji 4. kandydaci do pracy 5. użytkownicy strony internetowej 6. klienci (przedstawiciele klienta) - osoby fizyczne 7. potencjalni klienci (przedstawiciele potencjalnego klienta) - osoby fizyczne 8. kontrahenci (dostawcy) - osoby fizyczne prowadzące działalność gospodarczą 9. osoby reprezentujące kontrahentów (dostawców) 10. pracownicy 11. osoby współpracujące na podstawie umowy zlecenia / umowy o dzieło	
4.	**Proszę opisać kategorie danych osobowych, które mają być wykorzystane w Projekcie**	Jakie dane osób będą przetwarzane w projekcie osobach wskazanych powyżej? (pkt 3) Przykładowo: 1. studenci - imię i nazwisko, numer telefonu, adres email 2. wykładowcy – adres i email 3. kontrahenci - imię i nazwisko, adres siedziby, NIP Kategorie danych osobowych to np.: imię, nazwisko, adres IP, pliki cookies, linie papilarne, numery ID, wizerunek twarzy/osoby (w tym dane z monitoringu), dane o lokalizacji, numer VIN, numer rachunku bankowego, adres zamieszkania, adres zameldowania, nr dowodu osobistego, nr paszportu, nr prawa jazdy, PESEL, NIP, REGON, wykształcenie, zawód, stanowisko, stan rodzinny, imiona rodziców, sygn. akt / nr decyzji w przypadku orzeczeń sądowych, administracyjnych, jednostki chorobowe, nałogi, informacji o aktywności użytkownika strony internetowej, informacje o przebiegu współpracy (np. historia zamówień). **UWAGA!** **Jeśli dane mają być przetwarzane w systemie IT, skonsultuj się z działem IT i potwierdź, czy zakres danych, który wskazałeś jest wyczerpujący. Jeśli nie - należy uzupełnić opis o dane wskazane przez dział IT.**	
5.	**Czy Projekt jest skierowana do osób w wieku poniżej 16 lat lub dane dzieci poniżej 16 r.ż. będą wykorzystywane w procesie?**		
6.	**Skąd pochodzą dane, które mają być wykorzystywane w Projekcie?**	Proszę wskazać źródło pochodzenia danych – skąd pochodzą dane: a) osoba będzie podawała dane samodzielnie b) kto inny będzie podawał dane tej osoby c) dane będą zbierane na podstawie obserwacji aktywności tej osoby d) wykorzystywane będą dane już posiadane przez ADO. UWAGA! Jeśli część danych będzie np. zbierana na podstawie obserwacji aktywności osoby (c), a	

		część będzie podawała samodzielnie (a) należy wskazać: a) imię, nazwisko, adres - samodzielnie c) preferencje zakupowe, lokalizacja - z obserwacji aktywności	
7.	**Czy realizując Projekt dojdzie do powierzenia przetwarzania danych osoboych? Czy w celu realizacji Projektu korzystasz z podwykonawców?**	**TAK** - realizując Projekt korzystam z zewnętrznych podwykonawców, którzy będą przetwarzać dane osobowe i wykonywać czynności, w zakresie określonym przez ADO (w imieniu ADO i na jej polecenie). **NIE** - realizując Projekt nie korzystam z podwykonawców, wszystko jest wykonywane samodzielnie i wewnętrznie w ADO **Przykładowe sytuacje przy odpowiedzi TAK:** 1. dane osobowe studentów (osób fizycznych prowadzących działalność gospodarczą) są przekazywane firmie zewnętrznej w celu rozliczenia stypendiów 2. dane osobowe wykorzystywane w procesie są przechowywane na zewnętrznych serwerach lub w chmurze obliczeniowej (cloud computing) 3. ADO korzysta z zewnętrznego biura rachunkowego (przekazuje w celu dokonania rozliczenia dane pracowników itp.) 4. ADO korzysta z usług zewnętrznej agencji marketingowej, której przekazuje dane subskrybentów newslettera PWSZ. **UWAGA!** **Podwykonawcy nie mogą wykorzystywać danych osobowych do własnych celów (wyłącznie ADO może decydować, w jakim celu i w jaki sposób podwykonawca / zleceniobiorca wykorzystuje dane).**	
8.	**Czy podczas realizacji Projektu dane będą, udostępniane (przekazywane) innym podmiotom wykorzystującym dane dla własnych celów (niezwiązanych z potrzebami/celami ADO?**	TAK - dane będą przekazywane (ujawniane) innym podmiotom, które nie realizują żadnych działań na rzecz ADO oraz będą przetwarzać dla własnych celów. NIE - nikomu nie udostępniamy danych, wyłącznie pracownicy ADO oraz jej podwykonawcy mają dostęp do danych Przykładowo *udostępnić dane można podmiotom takim jak: organy podatkowe, firmy windykacyjne, prokuratura, ubezpieczyciel, sąd* Przykładowo *udostępnianie danych może mieć miejsce:* 1. dla organizacji z UE w związku z regulacją UE 2. dla Instytucji finansującej studenta 3. *gdy sąd żąda udostępnienie nagrania z monitoringu w związku z prowadzonym postępowaniem* 4. *jeśli ADO sprzedaje bazę danych zawierającą dane osobowe klientów innym podmiotom, które wykorzystują dane dla realizacji swoich kampanii reklamowych*	
9.	**Czy Projekt zakłada tworzenie profili na podstawie danych osobowych?**	Profilowanie występuje, jeśli spełnią się oba poniższe warunki: - dane osobowe są przetwarzane za pomocą systemów informatycznych - dokonywana jest analiza lub prognoza zachowań lub preferencji na podstawie tych danych. *Przykładowo:* *Po zebraniu danych kandydata na studia za pomocą narzędzia analitycznego analizowana jest jego miejsce zamieszkania, płeć, przeglądane treści i na tej podstawie tworzony jest jego*	

		profil, z którego wynika, że skoro jest kobietą mieszkającym we Wrocławiu w wieku 45 -55lat, która zakupiła 2 książki związane z tematyką farmacji , to będzie zainteresowana studiami podyplomowymi o kierunku z tym związanym	
10.	**Zautomatyzowane podejmowanie decyzji**	TAK - jeśli w ramach Projektu podejmowane są decyzje w oparciu o analizę danych określonej osoby i spełnione są wszystkie poniższe warunki: 1. dane są przetwarzane wyłącznie w systemach informatycznych 2. brak udziału człowieka w podejmowaniu decyzji (system sam analizuje dane i zwraca wynik) lub udział człowieka jest nieistotny, np. polega na wpisaniu danych do systemu 3. decyzja ma skutek prawny lub równie istotny, np. wpływa na możliwości zarobkowania (awans pracownika), przyznanie stypendium socjalnego (odmowa stypendium).	
11.	**Czy w związku z realizacją Projektu dane osobowe mogą być przekazywane poza terytorium Europejskiego Obszaru Gospodarczego (EOG)?**	Przykłady sytuacji TAK: Do przekazywania danych poza EOG może dochodzić, gdy np.: 1. *Uczelnia współpracuje w ramach międzynarodowych Konferencji,* 2. *ADO wysyła pracowników w podróże służbowe do państwa spoza EOG (np. przekazuje dane hotelom, przewoźnikom lotniczym)* 3. *ADO korzysta z rozwiązań chmurowych (cloud computing) podmiotów, których serwery znajdują się poza EOG* (W skład EOG wchodzą państwa Unii Europejskiej i Norwegia, Islandia oraz Liechtenstein)	
12.	**Jak długo potrzebujesz mieć dostęp do danych?**	**Przykładowo:** *- do zakończenia rekrutacji* *- do zakończenia konkursu* *- do zakończenia kampanii reklamowej* *- nie przewiduję kasowania danych* **UWAGA NALEŻY UZWGLĘDNIAĆ ASPEKTY PODATKOWE I EWENTUALNYCH ROSZCZEŃ CYWILNOPRAWNYCH** - w razie potrzeby konsultacja z Działem Prawnym	
13.	**Czy założenia Projektu uwzględniają zasadę minimalizacji danych osobowych?**	Zasada minimalizacji danych oznacza, że w ramach Projektu powinny być przetwarzane tylko te dane osobowe, które są niezbędne do zrealizowania jego celu/celów. *Przykład: Ocenianą Projektem jest wdrożenie w ramach zakupowej platformy intemetowej możliwości zakładania konta użytkownika w bibliotece PWSZ (oraz udostępnianie za jego pośrednictwem określonych funkcjonalności). Zgodnie z założeniem Projektu w celu założenia konta użytkownik powinien podać nr PESEL oraz informacje o stanie cywilnym, mimo że zbieranie takich informacji nie jest niezbędne do świadczenia usługi. Takie założenia należy ocenić jako błędne, ponieważ możliwe jest świadczenie planowanej usługi w przypadku zbierania mniejszej ilości danych o użytkowniku.*	
14	**Czy założenia Projektu uwzględniają zasadę**	Zasada domyślnej ochrony danych (privacy by default) wymaga zastosowania domyślnych	

	domyślnej ochrony prywatności?	mechanizmów//ustawień (w szczególności w przypadku Projekt zakładających przetwarzanie danych osobowych przy pomocy systemu/aplikacji) zapewniających możliwie najszerszą ochronę prywatności wszystkich podmiotów danych. Zaleca się model opt-in, co oznacza, że osoby, które chcą ograniczyć swoją prywatność (tj. zezwolić na dostęp do swoich danych), muszą podjąć aktywne działania w tym kierunku (np. zmienić ustawienia w aplikacji tak, aby zbierane i udostępniane innym osobom były dodatkowe informacje, które nie są niezbędne do realizacji Projektu).	
15.	**Czy założenia Projektu uwzględniają zasadę ograniczenia czasowego?**	Zasada ograniczenia czasowego oznacza, że dane powinny być przechowywane tylko przez taki okres, który jest niezbędny do realizacji celu Projektu. 1. Po tym okresie dane powinny być usuwane lub anonimizowane (tj. pozbawiane cech pozwalających na przypisanie ich do konkretnej osoby fizycznej). 2. Już w założeniach Projektu powinno się uwzględnić terminy usunięcia danych.	
16.	**Czy założenia Projektu uwzględniają Konieczność informowania o celach i sposobach przetwarzania danych i zasadę transparentności?**	Zasada transparentności wymaga informowania każdej osoby, której dane dotyczą o: 1. celach, 2. zakresie 3. sposobach przetwarzania danych osobowych. Projekt nie może zakładać, że część operacji na danych osobowych będzie wykonywana w tajemnicy przed podmiotem danych.	

Załącznik nr 4 do Polityki Ochrony Danych Osobowych

Legnica, dnia ..... r.

AKCEPTUJĘ:

.....
(Rektor/Kanclerz)

Wniosek
o (przyznanie/zmianę/wycofanie[1])
Uprawnień
do przetwarzania danych osobowych
Nr .....

dla Pani/Pana:

.....
(imię i nazwisko)

zatrudnionej/nego na stanowisku .....

w ..... pomieszczenie ...../...../.....
(nazwa jednostki/komórki organizacyjnej) (obiekt/budynek/nr)

do przetwarzania danych osobowych, które obejmuje/obejmowało[1] przetwarzanie

w zakresie .....
(wymienić rodzaj danych)

w[2].....

login[3]: .....

na okres od ..... do .....

.....
(podpis ASI)

.....
(podpis Wnioskodawcy)

[1]) podkreślić właściwe
[2]) podać sposób przetwarzania danych np. w systemie informatycznym (podać nazwę systemu) lub/także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych (wymienić)
[3]) (identyfikator użytkownika w systemie informatycznym) w przypadku nowego pracownika, po zatwierdzeniu Wniosku przez Rektora login do systemu informatycznego zakłada ASI, w przypadku zmian login podaje osoba dla której składany jest wniosek

Załącznik nr 5 do Polityki Ochrony Danych Osobowych

Legnica, dnia ..... r.

Upoważnienie
do przetwarzania danych osobowych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy

nr .....

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 Nr 119, s. 1) – nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(nazwa jednostki/komórki organizacyjnej)

do przetwarzania danych osobowych PWSZ im. Witelona w Legnicy zgodnie z Wnioskiem nr ....., na okres od .....do ..... oraz zobowiązuje do przetwarzania danych osobowych zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r., wydanymi na jego podstawie aktami wykonawczymi oraz obowiązującymi przepisami wewnętrznymi.

.....
(Rektor/Kanclerz)

.....
(data i podpis IOD)

.....
(data i podpis upoważnionego)

Upoważnienie wycofano dnia: .....

.....
(data i podpis IOD)

Wzór rejestru upoważnień

Nazwisko	Imię	Komórka organizacyjna	Zakres uprawnień	Login	Numer upoważnienia	Data nadania uprawnień	Data wycofania uprawnień

Załącznik nr 7 do Polityki Ochrony Danych Osobowych

OŚWIADCZENIE

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz obowiązującymi przepisami wewnętrznymi.

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach;
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora;
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora;
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....

(podpis osoby upoważnionej)

KARTA SZKOLENIA WSTĘPNEGO
Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Imię i nazwisko osoby odbywającej szkolenie: Stanowisko:
Instruktaż przeprowadził w dniu: _____ (imię i nazwisko przeprowadzającego instruktaż)
W ramach szkolenia, na bazie prezentacji oraz w odniesieniu się do: a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), b) dokumentacji związanej z ochroną danych osobowych (Polityka Ochrony Danych Osobowych) przyjętej przez ADO
Poruszone zostały następujące tematy i zagadnienia: 1. Podstawowe pojęcia (dane osobowe, przetwarzanie danych osobowych, zasady przetwarzania danych osobowych, administrator danych, podmiot przetwarzający, osoba upoważniona, podstawy przetwarzania danych osobowych, prawa osób których dane dotyczą). 2. Upoważnienie do przetwarzania danych. 3. Obowiązek informacyjny zgodnie z art. 13-14 RODO. 4. Incydenty naruszenia bezpieczeństwa danych osobowych, naruszenie ochrony danych osobowych. 5. Obowiązki przy przetwarzaniu danych – projektowanie ochrony danych. 6. Zasady bezpiecznego przetwarzania danych osobowych w PWSZ. 7. Pomieszczenia, które są zamykane na klucz i w których są przetwarzane dane osobowe powinny być zamykane na klucz. Dostęp do kluczy posiadają tylko upoważnieni pracownicy. 8. Szafy w których przechowywane są dane, szczególnie dokumentacja studentów, pracowników, powinny być zamykane na klucz. Klucze do tych szaf posiadają tylko upoważnieni pracownicy. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane. 9. Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf. Zakazane jest przechowywanie akt osobowych pracowników, dokumentacji pracowniczej lub innych danych osobowych w tym danych studentów w sposób niezabezpieczony. 10. Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy. 11. Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane. 12. W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane. 13. Nie należy udostępniać osobom nieupoważnionym dostępu do komputerów i laptopów. 14. Nośniki pamięci przenośnej np. pendrive albo pliki na nich zawarte należy szyfrować. Po użyciu danych, należy pamięć przenośną wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe. 15. Plików zawierających dane osobowe (w skanach, plikach word lub exel lub w innych formatach) i których ujawnienie może powodować ryzyko naruszenia praw i wolności osób fizycznych, szczególnie wyników badań, dokumentacji medycznej nie należy przesyłać drogą elektroniczną w sposób niezabezpieczony. 16. Dokumenty zawierające dane osobowe po ich wydrukowaniu należy niezwłocznie odbierać z drukarek. 17. Incydenty naruszenia bezpieczeństwa informacji należy zgłaszać bezpośrednio przełożonemu niezwłocznie po ich wykryciu. 18. Pracownik/Współpracownik ma obowiązek pamiętać że Pracodawca ma 72 godziny od momentu ujawnienia incydentu na powiadamianie o tym organu nadzoru Prezesa Urzędu Ochrony Danych Osobowych. 19. Należy wspierać Pracodawcę w wykonywaniu obowiązku bezpiecznego przetwarzania danych osobowych.
Wskazano kwestie odpowiedzialności za przetwarzanie danych osobowych oraz za prawidłowy nadzór przetwarzania danych osobowych. Poinformowano, że za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność dyscyplinarna, odszkodowawcza, a w skrajnych przypadkach nawet karna.
Podkreślono znaczenie i rolę osób upoważnionych w szczelności systemu ochrony danych osobowych. Szczególny nacisk położono na należytą uwagę i rozwagę w przetwarzaniu danych osobowych o zdrowiu, w szczególności co do konsekwencji jakie może ponieść ADO za nienależytą staranność osoby upoważnionej przy przetwarzaniu danych osobowych i niewypełnianiu obowiązków wynikających z RODO.
Przypadki kwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie: 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych jak np.: pożar, zalanie pomieszczeń. 2) naruszenie lub próba naruszenia integralności systemu lub bazy danych, 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru, 4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu, 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną

nadzwyczajną i niepożądaną modyfikację w systemie,
6) ujawnienie haseł do sytemu IT,
7) stwierdzenie próby lub modyfikacji danych lub zmian w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych,
10) zagubienie teczki osobowej studenta, pracownika itp.
11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa danych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, ksero, nie zamknięcie pomieszczenia w którym znajdują się dokumenty zawierające dane osobowe nie zabezpieczone w inny sposób, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).
14)za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

TEKST NINIEJSZY ZOSTAŁ PRZEZE MNIE PRZECZYTANY, W PEŁNI ZROZUMIANY I ZAAKCEPTOWANY. ZOBOWIĄZUJĘ SIĘ GO PRZESTRZEGAĆ, CO POTWIERDZAM WŁASNORĘCZNYM PODPISEM.

.....

(data i podpis osoby, której udzielono instruktażu)

Legnica dn.....r.

UPOWAŻNIENIE
DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Dz. Urz. UE L 119 z dnia 04.05.2016 r.,

upoważniam Panią/Pana:

.....

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania

- ☐ obowiązków służbowych
- ☐ prac zleconych
- ☐ szczegółowych zadań, jak .....

.....

(podpis ADO)

Legnica, dnia .....r.

.....

(imię i nazwisko pracownika)

.....

(stanowisko)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz wewnętrznymi przepisami dotyczącymi .

W szczególności zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności zleconych*
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych a następnie przekazanie ich do dyspozycji osób upoważnionych
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Pracodawcę za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....

podpis oświadczającego

** za czynności zlecone w obszarze przetwarzania danych osobowych rozumie się w szczególności: sprzątanie pomieszczeń, ochrona obiektów i pomieszczeń, konserwacja infrastruktury znajdującej się w obszarze przetwarzania danych osobowych*

Wzór rejestru czynności przetwarzania danych

Opis kategorii osób, których dane dotyczą (nazwa zbioru)	
Rejestr czynności przetwarzania?	
Ocena skutków?	

Imię i nazwisko, nazwa oraz dane kontaktowe: Administratora (Przedstawiciela administratora) / Współadministratorów / Podmiotu przetwarzającego	
Cele przetwarzania	
Opis kategorii danych osobowych	
Zakres danych, charakter, kontekst	
Adekwatność danych (art. 5 ust. 1 lit. c)	
Zgodność przetwarzania z prawem (art. 6, 9)	
Czas przetwarzania - planowane terminy usunięcia poszczególnych kategorii danych	
Realizowanie praw osób, których dane dotyczą	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Nazwa państwa trzeciego lub organizacji międzynarodowej, do której przekazywane są dane i wskazanie dokumentacji odpowiednich zabezpieczeń	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	
Relacje z podmiotem przetwarzającym (art. 28)	
Funkcjonalny opis operacji przetwarzania	

Aktywa

1. Informacje (wersja papierowa)	
2. Programy i systemy operacyjne	
3. Infrastruktura IT	
4. Infrastruktura	
5. Pracownicy i współpracownicy	
6. Outsourcing	

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

1. Pracownik odpowiedzialny za organizację konferencji naukowej lub innego wydarzenia, zobowiązany jest w imieniu Administratora danych osobowych do spełnienia obowiązku informacyjnego wynikającego z obowiązujących przepisów prawa, w szczególności:
    1) do zamieszczenia obowiązkowych klauzul informacyjnych w materiałach promujących konferencję naukową lub inne wydarzenie, we wszelkich formach informacji (w tym na stronach internetowych), jeżeli w związku z organizacją konferencji naukowej lub innego wydarzenia następować będzie przetwarzanie danych osobowych. Wzór klauzuli informacyjnej Administratora danych osobowych stanowi Załącznik 7 do niniejszej Polityki bezpieczeństwa informacji w zakresie danych osobowych.
    2) do pozyskania oświadczenia w przedmiocie udzielenia zgody na przetwarzanie danych osobowych od osób, których dane osobowe będą przetwarzane dla celów organizacji konferencji lub innego wydarzenia.
2. Zamieszczanie danych biometrycznych w postaci wizerunku osób na stronach internetowych należących do Administratora danych lub materiałach promocyjnych i folderach reklamowych Administratora danych wymaga uzyskania pisemnej zgody na przetwarzanie danych, zawierającej wyraźne oświadczenie o wyrażeniu zgody na korzystanie z wizerunku, jego publikację oraz przetwarzanie danych biometrycznych osoby, której zgoda dotyczy.
3. Obowiązek pozyskania zgody na publikację wizerunku nie dotyczy osób powszechnie znanych w związku z pełnieniem przez nich funkcji publicznych, w szczególności politycznych, społecznych, zawodowych.
4. Obowiązek pozyskania zgody na publikację wizerunku nie dotyczy osoby stanowiącej jedynie szczegół całości takiej, jak zgromadzenie, krajobraz, publiczna impreza.
5. Wzór oświadczenia w przedmiocie udzielenia zgody na przetwarzanie danych osobowych przygotowuje osoba odpowiedzialna za organizację konferencji/wydarzenia konsultując wzór z IOD. Wzór oświadczenia musi zostać opracowany każdorazowo dla danego wydarzenia, z uwzględnieniem specyfiki wydarzenia, z rozdzieleniem czynności i celów przetwarzania.
6. Pracownicy Administratora danych przetwarzają dane osobowe dla celów konferencji naukowej lub innego wydarzenia organizowanego przez Administratora danych wyłącznie na podstawie stosownych upoważnień do przetwarzania danych osobowych i zgodnie z obowiązującymi przepisami prawa powszechnie obowiązującego oraz aktów wewnętrznych.

PROCEDURA OBSŁUGI PRAW PODMIOTÓW DANYCH

§ 1.
Cel Procedury

1. Niniejsza procedura ustanawia ramy dla osiągnięcia zgodności z RODO Uczelni w zakresie realizacji praw podmiotów, których dane dotyczą.
2. Niniejszą procedurę należy stosować gdy osoba, której dane dotyczą, wykonuje jedno lub więcej praw przysługujących jej na mocy RODO.
3. Uczelnia stosuje proaktywne podejście w celu realizacji żądań osób, których dane dotyczą, które zapewni jak największą kontrolę nad danymi osobowymi w rękach podmiotu danych, przy minimalnej interwencji lub zaangażowaniu wymaganym ze strony Uczelni.

§ 2.
Ogólne zasady dotyczące obsługi wniosku/żądania podmiotu danych

1. Wnioski/żądania osób, których dane dotyczą rozpatrywać należy indywidualnie. IOD decyduje, czy dane żądanie lub wniosek możliwe jest do realizacji czy nie, na podstawie analizy każdego przypadku w oparciu o przepisy praw oraz niniejsza Procedurę.
2. Nadzór nad realizacją zadań wynikających z niniejszej procedury w poszczególnych komórkach sprawuje IOD.
3. Uczelnia ułatwia osobom korzystanie z ich praw poprzez różne działania, takie jak zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób i sposobie korzystania z nich, w tym metodach kontaktu w tym celu.
4. Uczelnia dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób i wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. W celu ułatwienia realizacji praw podmiotu danych IOD może ustalić formularz realizacji praw.
6. Każdy pracownik Uczelni ma obowiązek niezwłocznego przekazania wniosku podmiotu danych dotyczącego realizacji praw z RODO do IOD.
7. Wszelkie informacje, pisma przekazywane są podmiotowi danych w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Informacje lub pisma mogą być przekazywane do osoby, której dane dotyczą na piśmie, w formie elektronicznej lub w inny sposób.
8. Osoba, której dane dotyczą, może zażądać informacji w formie pisemnej lub elektronicznej albo ustnie (np. przez telefon lub osobiście). Jeżeli osoba, której dane dotyczą zażąda ustnego udzielenia informacji, można takich udzielić pod warunkiem, że innymi sposobami uda się potwierdzić tożsamość osoby, której dane dotyczą. W przypadku żądania przekazanego ustnie lub osobiście, fakt taki należy odnotować w rejestrze wniosków/żądań podmiotu danych i niezwłocznie go potwierdzić w formie notatki służbowej zawierającej określenie tożsamości podmiotu danych, datę zgłoszenia wniosku/żądania oraz jego treść. Notatka może zostać zastąpiona emailem wysłanym na adres poczty elektronicznej podmiotu danych, o ile Uczelnia taki przetwarza.
9. Przed realizacją każdego wniosku/żądania należy potwierdzić tożsamość osoby, której dane dotyczą w celu upewnienia się, że z żądaniem występuje osoba, której dane dotyczą. W razie uzasadnionych wątpliwości co do tożsamości osoby fizycznej składającej żądanie, przed udzieleniem odpowiedzi właściciel procesu może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
10. Uczelnia odpowiada na wniosek/żądanie osoby, której dane dotyczą bez zbędnej zwłoki i w ciągu maksymalnie jednego miesiąca od otrzymania wniosku/żądania. W odpowiedzi informuje się o działaniach podjętych w związku z żądaniem.
11. W razie odmowy spełnienia całości lub części żądania, w odpowiedzi informuje się o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
12. W razie skomplikowanego charakteru żądania lub zbyt dużej liczby żądań, termin na udzielenie informacji o działaniach podjętych w związku z żądaniem można przedłużyć o kolejne dwa miesiące, o ile w terminie miesiąca od dnia wpływu żądania, osoba, której dane dotyczą, otrzyma informację o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
13. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter Administrator może:
    1) skonsultować pobór rozsądnej opłaty z IOD, lub
    2) odmówić spełnienia całości lub części żądania, o ile w razie sporu Uczelnia będzie w stanie wykazać, że żądanie miało ewidentnie nieuzasadniony lub nadmierny charakter.
14. Jeżeli wniosek jest składany za pomocą formularza elektronicznego, odpowiedź powinna być przekazywana drogą elektroniczną, o ile jest to możliwe i o ile podmiot danych nie wnioskuje inaczej.
15. Osoba upoważniona do przetwarzania danych osobowych odnotowuje fakt realizacji praw podmiotów danych w systemie, który służy do przetwarzania danych osobowych (np. system kadrowo-płacowy).

16. Należy zadbać o udokumentowanie zrealizowania odpowiedzi na wniosek/żądanie osoby, której dane dotyczą w terminie np. poprzez wysłanie emaila z żądaniem potwierdzenia jego otrzymania, przesłanie odpowiedzi listem za potwierdzeniem nadania.
17. Uczelnia informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw (Nieprzetwarzanie).
18. Uczelnia w zakresie w jakim wykonuje zadania publiczne nie przekazuje informacji, o których mowa w art. 13 ust. 3 RODO jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 13 ust. 3 RODO, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 tego rozporządzenia, oraz przekazanie tych informacji:
    1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
    2) naruszy ochronę informacji niejawnych.
19. Uczelnia w zakresie w jakim wykonuje zadania publiczne nie przekazuje informacji, o których mowa w art. 14 ust. 1, 2 i 4 RODO jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w art. 14 ust. 1, 2 i 4 RODO jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 RODO, oraz przekazanie tych informacji:
    1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
    2) naruszy ochronę informacji niejawnych.
20. Uczelnia w zakresie w jakim wykonuje zadania publiczne nie przekazuje informacji o których mowa w art. 15 ust. 1–3 RODO, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązków, o których mowa w art. 15 ust. 1–3 RODO, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 RODO oraz wykonanie tych obowiązków:
    1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
    2) naruszy ochronę informacji niejawnych.
21. W przypadku, o którym mowa w ust. 18, ust. 19, Uczelnia zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. Uczelnia jest obowiązana poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 13 ust. 3 RODO.
22. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 RODO wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, Uczelnia wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. W takiej sytuacji Uczelnia zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w art. 15 ust. 1–3 RODO

§ 3.
Realizacja obowiązku informacyjnego

1. Uczelnia określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych i w tym celu:
    1) Informuje osobę o przetwarzaniu jej danych już na etapie pozyskiwania danych od tej osoby (przekazuje klauzulę informacyjną zgodnie ze wzorem ustalonym przez ADO)
    2) Informuje osobę o przetwarzaniu jej danych w przypadku pozyskania danych w sposób inny niż od osoby, której dane dotyczą.
    3) Określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
    4) Informuje osobę o planowanej zmianie celu przetwarzania danych oraz o planowanym uchyleniu ograniczenia przetwarzania.
    5) Informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
    6) Informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
    7) Bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby
    8) informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
2. W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadamiać o prawie do odwołania takiej zgody.

3. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO. Za stosowanie właściwych klauzuli informacyjnych przy zbieraniu danych osobowych odpowiada każdy pracownik.
4. Administrator może ustalić obowiązujące wzory klauzul informacyjnych dla poszczególnych procesów przetwarzania danych realizowanych przez Uczelnię. Wzory klauzul informacyjnych dostępne są u IOD. Wszelkie zmiany klauzul informacyjnych wymagają konsultacji z IOD.
5. W przypadku zbierania danych od osoby, której dane dotyczą, podczas pozyskiwania danych osobowych podaje się informacje, o których mowa w art. 13 RODO, chyba że osoba, której dane dotyczą dysponuje już tymi informacjami.
6. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, osobie, której dane dotyczą, podaje się informacje, o których mowa w art. 14 RODO. Obowiązek podania informacji nie ma zastosowania, gdy:
   1) osoba której dane dotyczą, dysponuje już tymi informacjami,
   2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
   3) proces pozyskiwania danych jest wyraźnie uregulowany prawem Unii Europejskiej lub prawem państwa członkowskiego, lub
   4) dane muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
7. Informacji, o których mowa w ust. 6, udziela się:
   1) w rozsądnym terminie po pozyskaniu danych osobowych, najpóźniej w ciągu miesiąca, mając na uwadze konkretne okoliczności przetwarzania danych osobowych,
   2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą, lub
   3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
8. Przed dalszym przetwarzaniem danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, osobie, której dane dotyczą podaje się ten sam zakres informacji, co przy zbieraniu danych.

§ 4.
Realizacja poszczególnych praw podmiotów danych

[prawo do cofnięcia zgody]

1. Osoba, której dane dotyczą, ma prawo do wycofania zgody (prawo do cofnięcia zgody), jeżeli podstawą przetwarzania ich danych osobowych jest zgoda. Cofnięcie zgody ma skutek od momentu wycofania zgody. Cofnięcie zgody nie wpływa na przetwarzanie dokonywane przez nas zgodnie z prawem przed jej cofnięciem. Przed realizacją prawa do cofnięcia zgody należy potwierdzić, że zgoda jest rzeczywiście podstawą przetwarzania. Jeżeli dane przetwarzanie nie wymaga zgody podmiotu danych, należy odmówić realizacji żądania w zakresie w jakim istnieją inne podstawy do przetwarzania danych osobowych na innej podstawie (np. obowiązek prawny) i poinformować o tym osobę, której dane dotyczą.

[prawo dostępu do danych i wydania kopii danych]

2. Osoba, której dane dotyczą ma prawo uzyskać od Uczelni potwierdzenie, czy przetwarza jej dane osobowe, a jeżeli ma to miejsce, ma prawo (prawo dostępu do danych osobowych) uzyskać:
   1) dostęp do swoich danych osobowych;
   2) informacje o celach przetwarzania, kategoriach przetwarzanych danych osobowych, o odbiorcach lub kategoriach odbiorców tych danych, planowanym czasie przechowywania danych lub o kryteriach ustalania tego okresu, o prawach przysługujących na mocy RODO oraz o prawie wniesienia skargi do organu nadzorczego, o źródle tych danych, o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz o zabezpieczeniach stosowanych w związku z przekazaniem tych danych poza Unię Europejską;
   3) kopię swoich danych osobowych.
3. Jeżeli osoba fizyczna w ramach prawa dostępu zażąda informacji na temat przetwarzania dotyczących jej danych osobowych, należy udzielić jej informacji, o których mowa w art. 15 ust. 1 i 2 RODO, chyba że udzielenie takich informacji stałoby w sprzeczności z prawem Unii Europejskiej lub prawem państwa członkowskiego, w szczególności z ustawowym obowiązkiem zachowania tajemnicy.
4. Na żądanie osoby, której dane dotyczą, dostarcza się jej kopię danych osobowych podlegających przetwarzaniu, chyba że jej dostarczenie stałoby w sprzeczności z prawem Unii Europejskiej lub prawem państwa członkowskiego, w szczególności z ustawowym obowiązkiem zachowania tajemnicy. Sposób realizacji takiego żądania nie może wpływać niekorzystnie na prawa i wolności innych osób, a w szczególności nie może wiązać się z ujawnieniem dotyczących ich danych. Jeżeli osoba, której dane

dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, kopię przekazuje się powszechnie stosowaną drogą elektroniczną.

5. Fakt wydania kopii danych jest odnotowywany w rejestrze wniosków/żądań podmiotu danych. Kompilacja informacji w celu wydania kopii danych prawdopodobnie wymagać będzie współpracy kilku komórek organizacyjnych Uczelni.

[Prawo do przenoszenia danych]

6. Na żądanie podmiotu, którego dane dotyczą Uczelnia wydaje dane dotyczące tej osoby, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (xls,csv) lub przekazuje innemu administratorowi wskazanemu przez podmiot, którego dane dotyczą, jeżeli żądanie dotyczy danych zebranych od osoby, której dane dotyczą i pod warunkiem, że przetwarzanie:
   1) odbywa się na podstawie zgody osoby której dane dotyczą,
   2) odbywa się na podstawie umowy, której stroną jest osoba, której dane dotyczą,
   3) odbywa się w sposób zautomatyzowany, w szczególności poprzez serwis internetowy.
7. Przesłanie danych innemu podmiotowi – następuje pod warunkiem, że istnieją w tym zakresie techniczne możliwości zarówno po stronie Uczelni, jak i podmiotu wskazanego przez osobę, której dane dotyczą.

[prawo do sprostowania i uzupełnienia]

8. Jeżeli dane osobowe są niedokładne, podmiot danych ma prawo zażądać poprawienia i uzupełnienia niepełnych danych osobowych w oparciu o informacje, które mogą one dostarczyć.
9. W razie potrzeby IOD podejmie kroki w celu zweryfikowania informacji dostarczonych przez osobę, której dane dotyczą, w celu upewnienia się, że jest ona poprawna przed jej wprowadzeniem.
10. Na żądanie osoby, której dane dotyczą, dokonuje się niezwłocznego sprostowania nieprawidłowych danych osobowych. W przypadku sprostowania danych IOD informuje osobę o odbiorcach danych, na żądanie tej osoby.
11. IOD lub osoba przez niego wskazana uzupełnia i aktualizuje dane na żądanie osoby. Uczelnia ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. nie musi przetwarzać danych, które są jej zbędne). Uczelnia może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Uczelnię procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
12. Na żądanie osoby, której dane dotyczą, dokonuje się niezwłocznego uzupełnienia niekompletnych danych osobowych, chyba że żądany zakres danych osobowych nie będzie adekwatny do celów, w których dane są przetwarzane.

[prawo do usunięcia, do bycia zapomnianym]

13. Osoba, której dane dotyczą, ma prawo zażądać od Uczelni usunięcia danych osobowych na jej temat bez zbędnej zwłoki. Na żądanie podmiotu, którego dane dotyczą, Uczelnia usuwa dane, gdy:
   1) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
   2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   4) dane były przetwarzane niezgodnie z prawem,
   5) konieczność usunięcia wynika z obowiązku prawnego,
   6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).
14. Należy odmówić rozpatrzenia wniosku jeżeli przetwarzanie jest niezbędne:
   1) do korzystania z prawa do wolności wypowiedzi i informacji;
   2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego,
   3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
   4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
   5) do ustalenia, dochodzenia lub obrony roszczeń.
15. Uczelnia określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
16. Jeżeli dane podlegające usunięciu zostały upublicznione przez Uczelnię, Uczelnia podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane

osobowe o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Uczelnia informuje osobę o odbiorcach danych, na żądanie tej osoby.

17. Jeżeli osoba, której dane dotyczą, żąda niezwłocznego usunięcia danych osobowych (realizacji prawa do bycia zapomnianym), należy wypełnić formularz stanowiący **Załącznik 1** i postępować zgodnie z zawartymi w nim instrukcjami.

[prawo do ograniczenia przetwarzania danych]

18. Osoba, której dane dotyczą może skorzystać z prawa do ograniczenia przetwarzania swoich danych osobowych. Uczelnia dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
    1) osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość,
    2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    3) Uczelnia nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    4) podmiot, którego dane dotyczą wniósł sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu stwierdzenia, czy po stronie Uczelni zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
19. W trakcie ograniczenia przetwarzania Uczelnia przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje; nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Uczelnia zaprzestaje dokonywania operacji na danych osobowych, z wyjątkiem operacji, na które wyraziła zgodę osoba, której dane dotyczą, oraz ich przechowywania zgodnie z przyjętymi zasadami retencji lub dopóki nie ustaną przyczyny ograniczenia przetwarzania danych (np. zostanie wydana decyzji organu nadzorczego zezwalająca na dalsze przetwarzanie danych).
20. Uczelnia informuje osobę przed uchyleniem ograniczenia przetwarzania.
21. W przypadku ograniczenia przetwarzania danych Uczelnia informuje osobę o odbiorcach danych, na żądanie tej osoby.
22. Jeżeli osoba, której dane dotyczą, żąda ograniczenia przetwarzania danych osobowych, przetwarzanie tych danych zmienia się w następujący sposób:
    1) Jeżeli osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych, zawiesza się przetwarzanie danych osobowych do czasu weryfikacji prawidłowości tych danych, a w razie potrzeby ich sprostowania lub uzupełnienia – do czasu realizacji tych czynności.
    2) Jeżeli przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania, dalsze przetwarzanie prowadzi się zgodnie z tym żądaniem.
    3) Jeżeli organizacja nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń, dane osobowe przechowuje się przez okres objęty żądaniem.

[prawo do sprzeciwu]

23. Jeżeli osoba, której dane dotyczą wniosła sprzeciw, o którym mowa w art. 21 RODO, przetwarzanie danych osobowych zawiesza się do czasu rozpatrzenia sprzeciwu.
24. Sprzeciw w szczególnej sytuacji - Jeżeli osoba, której dane dotyczą zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Uczelnię w oparciu o uzasadniony interes Uczelni lub, o powierzone Uczelni zadanie, w interesie publicznym, Uczelnia uwzględni sprzeciw, o ile nie zachodzą po stronie Uczelni ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń. Sprzeciw w tym zakresie powinien zawierać uzasadnienie.
25. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Uczelnia prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Uczelnia uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Sprzeciw w tym zakresie powinien zawierać uzasadnienie.
26. Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Uczelnię na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Uczelnia uwzględni sprzeciw i zaprzestanie takiego przetwarzania. Sprzeciw przeciwko przetwarzaniu na potrzeby marketingu bezpośredniego nie musi zawierać uzasadnienia.
27. W razie wniesienia przez osobę, której dane dotyczą, sprzeciwu wobec przetwarzania dotyczącego jej danych osobowych:
    1) Jeżeli sprzeciw dotyczy przetwarzania danych, w tym profilowania, do celów marketingu bezpośredniego – należy niezwłocznie zaprzestać przetwarzania danych do takich celów.
    2) Jeżeli sprzeciw dotyczy przetwarzania danych do celów badań naukowych lub historycznych lub do celów statystycznych – należy niezwłocznie zaprzestać przetwarzania danych do takich celów, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

3) Jeżeli sprzeciw dotyczy przetwarzania danych, w tym profilowania, do celów wynikających z prawnie uzasadnionych interesów realizowanych przez organizację lub stronę trzecią, lub w celu wykonania zadania realizowanego w interesie publicznym – należy niezwłocznie zaprzestać przetwarzania, jeżeli interesy, prawa i wolności osoby, której dane dotyczą, są nadrzędne wobec prawnie uzasadnionych podstaw do przetwarzania.

28. Jeżeli sprzeciw nie dotyczy żadnej z sytuacji wymienionych w pkt 24-27 należy uznać go za bezzasadny. Oceniając zasadność sprzeciwu, należy przede wszystkim odpowiedzieć na pytanie, czy sprzeciw został wniesiony z przyczyn związanych ze szczególną sytuacją danej osoby.
29. W razie wpłynięcia żądania od osoby, której dane dotyczą, każda z osób upoważnionych do przetwarzania danych osobowych obowiązana jest niezwłocznie przekazać dane nadawcy i treść żądania właścicielowi procesu przetwarzania danych osobowych, wskazanemu w RCP. W razie wątpliwości, kto jest właścicielem procesu, należy skonsultować się z IOD.
30. Za odpowiadanie na żądania osoby, której dane dotyczą, odpowiedzialny jest kierownik komórki organizacyjnej, do której wpłynął wniosek, chyba że IOD przejmie udzielanie odpowiedzi. Jeżeli żądanie dotyczy danych przetwarzanych w ramach wielu procesów, każdy z właścicieli odpowiedzialny jest w zakresie, w jakim ma kontrolę nad przetwarzaniem danych, których dotyczy żądanie. W razie wątpliwości, czy dane osoby, której dotyczy żądanie, są przetwarzane także w innych procesach, właściciel procesu konsultuje się z przedstawicielem najwyższego kierownictwa lub inną osobą wyznaczoną do sprawowania nadzoru nad systemem ochrony danych osobowych.

3. KROKI PROCEDURY

KROK	OPIS	OSOBA ODPOWIEDZIALNA
Otrzymano żądanie podmiotu danych	Uczelnia ustala formularze wniosku o dane, jednak podmiot danych może zwrócić się z żądaniem w jakiejkolwiek wybranej przez siebie formie. Osoba, której dane dotyczą, składa wniosek za pomocą jednej z wielu metod, w tym drogą elektroniczną (pocztą elektroniczną lub za pośrednictwem naszej strony internetowej), listownie lub telefonicznie. Żądanie/wniosek podmiotu danych może zostać odebrany przez dowolną osobę ze Uczelni. Osoba otrzymująca wniosek/żądanie zobowiązana jest do jego niezwłocznego przekazania IOD.	
Rejestracja żądania podmiotu danych	Należy zarejestrować wniosek/żądanie podmiotu danych w rejestrze wniosków/żądań podmiotu danych prowadzonym przez IOD wraz z datą jego otrzymania przez UCZELNIĘ.	
Potwierdź tożsamość osoby, której dane dotyczą	Należy upewnić się, czy osoba występująca z danym wnioskiem/żądaniem to osoba, której dane dotyczą. W razie potrzeby można poprosić o więcej informacji, aby potwierdzić jej tożsamość. Jeśli tożsamość osoby, której dane dotyczą, nie może zostać potwierdzona, wniosek zostaje odrzucony. Następnie należy poinformować podmiot, który zgłosił się z danym wnioskiem/żądaniem o powodzie niezrealizowania wniosku/żądania oraz o przysługującym jej prawie do złożenia skargi do organu nadzorczego oraz możliwości skorzystania ze środków ochrony prawnej przed sądem.	

Oceń ważność wniosku	Należy sprawdzić, czy wniosek jest "oczywiście bezzasadny lub nadmierny". W przypadku wniosków o sprostowanie, usunięcie, ograniczenie lub sprzeciw wobec przetwarzania, zostaje podjęta decyzja, czy wniosek jest uzasadniony i zgodny z prawem. Jeśli nie, wniosek zostaje odrzucony. W takim przypadku należy poinformować osobę, której dane dotyczą o decyzji i o przysługującym jej prawie do złożenia skargi do organu nadzorczego oraz możliwości skorzystania ze środków ochrony prawnej przed sądem.	
Ustal czy żądanie ma ewidentnie nieuzasadniony lub jest nadmierne	Jeżeli podjęto decyzję o nałożeniu. należy osobę, której dane dotyczą poinformować o tym, że jej wniosek/żądanie zostanie zrealizowane po dokonaniu opłaty i przyczynach podjęcia takiej decyzji. Należy poinformować osobę, której dane dotyczą o tym, że ma możliwość podjęcia decyzji o dalszym popieraniu wniosku/ żądania lub jego cofnięcia . Jeżeli osoba, której dane dotyczą, postanowi nie kontynuować, wniosek zostanie odrzucony jeżeli nie zostanie dokonana opłata. W takim przypadku należy poinformować osobę, której dane dotyczą o decyzji i o przysługującym jej prawie do złożenia skargi do organu nadzorczego oraz możliwości skorzystania ze środków ochrony prawnej przed sądem.	
Skompletuj informacje	Należy zadbać o zebranie informacji, w tym przetwarzanych danych osobowych osoby, której dane dotyczą. Odpowiednie informacje są kompilowane zgodnie z rodzajem zapytania. Może to wymagać zaplanowania dokonania określonej czynności, np. usuniecie lub ograniczenie przetwarzania.	
Wykonaj żądanie podmiotu danych	Po skompletowaniu informacji lub w przypadku innego żądania należy je przesłać albo wykonać najpóźniej w terminie miesiąca od otrzymania wniosku/żądania przez Uczelnię.	
Zamknij żądanie/wniosek podmiotu danych	Fakt, że odpowiedź została rozpatrzona, jest rejestrowany w rejestrze wniosków/żądań podmiotu danych prowadzonym przez IOD wraz z datą zamknięcia.	

4. MONITOROWANIE I SZKOLENIA

1. Sposób realizacji niniejszej Polityki podlega weryfikacji w ramach corocznego sprawdzenia systemu ochrony danych osobowych.
2. Uczelnia dba o wdrażanie działań korygujących w celu doskonalenia przyjętej Procedury realizacji praw podmiotów danych,
3. W ramach szkoleń pracowników z zakresu ochrony danych osobowych należy położyć szczególny nacisk na kwestie ujęte w niniejszej Procedurze.

ZAŁĄCZNIK 1– FORMULARZ WERYFIKACJI ŻĄDANIA USUNIĘCIA DANYCH OSOBOWYCH (PRAWO DO BYCIA ZAPOMNIANYM)

FORMULARZ WERYFIKACJI ŻĄDANIA USUNIĘCIA DANYCH OSOBOWYCH	
Przesłanki zastosowania prawa do usunięcia danych	
Pytanie dotyczące danych objętych żądaniem usunięcia	**Odpowiedź (tak / nie)**
Czy dane nie są już niezbędne do celów, w których są przetwarzane?	
Czy osoba, której dane dotyczą, cofnęła zgodę na przetwarzanie danych i nie ma innej podstawy prawnej przetwarzania?	
Czy osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych, i sprzeciw ten jest zasadny z punktu widzenia ust. 36 i 37 Polityki ochrony danych osobowych?	
Czy na jakimkolwiek etapie przetwarzania, dane osobowe były przetwarzane niezgodnie z prawem?	
Czy obowiązek usunięcia wynika z przepisu prawa Unii Europejskiej lub prawa państwa członkowskiego?	
Czy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku?	
JEŻELI KTÓRAKOLWIEK Z ODPOWIEDZI NA POWYŻSZE PYTANIA BRZMI „TAK", NALEŻY WYPEŁNIĆ DALSZĄ CZĘŚĆ. JEŚLI NIE, PRAWO DO BYCIA ZAPOMNIANYM NIE MA ZASTOSOWANIA.	
Wyjątki od zastosowania prawa do usunięcia danych	
Pytanie dotyczące danych objętych żądaniem usunięcia	**Odpowiedź (tak / nie)**
Czy przetwarzanie jest niezbędne do korzystania z prawa wolności wypowiedzi i informacji?	
Czy przetwarzanie jest niezbędne do realizacji obowiązku wynikającego z przepisu prawa Unii Europejskiej lub prawa państwa członkowskiego?	
Czy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie	

publicznym lub w ramach sprawowania władzy publicznej powierzonej organizacji?	
Czy przetwarzanie jest niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO?	
Czy jest prawdopodobne, że usunięcie danych uniemożliwi lub poważnie utrudni przetwarzanie danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO?	
Czy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń?	
JEŻELI KTÓRAKOLWIEK Z ODPOWIEDZI NA POWYŻSZE PYTANIA BRZMI „TAK", DANE OSOBOWE NALEŻY USUNĄĆ JEDYNIE W TAKIM ZAKRESIE, W JAKIM ZIDENTYFIKOWANY WYJĄTEK NIE MA ZASTOSOWANIA.	
JEŻELI UCZELNIA UPUBLICZNIŁA DANE OSOBOWE, KTÓRE NALEŻY USUNĄĆ, TO NALEŻY W MIARĘ MOŻLIWOŚCI POINFORMOWAĆ ADMINISTRATORÓW PRZETWARZAJĄCYCH TE DANE OSOBOWE, ŻE OSOBA, KTÓREJ DANE DOTYCZĄ, ŻĄDA, BY ADMINISTRATORZY CI USUNĘLI WSZELKIE ŁĄCZA DO TYCH DANYCH, KOPIE TYCH DANYCH OSOBOWYCH LUB ICH REPLIKACJE. JEŚLI NIE MA INNEJ MOŻLIWOŚCI POINFORMOWANIA ADMINISTRATORÓW, INFORMACJĘ O ŻĄDANIU USUNIĘCIA DANYCH NALEŻY UMIEŚCIĆ W MIEJSCU, W KTÓRYM DANE TE BYŁY UPUBLICZNIONE.	

/……/

Podpis pracownika

POLITYKA RETENCJI DANYCH

§ 1.
Cel polityki

1. Niniejsza procedura jest elementem Polityki Ochrony Danych Osobowych w Uczelni.
2. Celem niniejszej Polityki jest spełnienie zasady minimalizacji i ograniczenia czasowego przetwarzania danych osobowych oraz określenie sposobu ustalania terminów usunięcia danych osobowych.
3. W każdej sprawie związanej z usuwaniem danych osobowych należy konsultować się z IOD.

§ 2.
Zakres stosowania i odpowiedzialność

1. Działania opisane w niniejszej procedurze obowiązują, we wszystkich komórkach organizacyjnych Uczelni.
2. Odpowiedzialność za prawidłowe ustalanie terminów przetwarzania danych osobowych spoczywa na kierownikach komórek organizacyjnych Uczelni.
3. Za przestrzeganie terminów usunięcia danych osobowych odpowiedzialni są kierownicy komórek organizacyjnych Uczelni, w zakresie, w jakim mają kontrolę nad przetwarzanymi danymi osobowymi w kierowanej komórce.

§ 3.
Ogólne zasady usuwania danych osobowych

1. Uczelnia przetwarza dane osobowe z uwzględnieniem zasady ograniczenia czasowego ich przechowywania i zapewnia że dane osobowe przetwarzane będą tylko tak długo jak długo przetwarzanie jest uzasadnione i zgodne z przepisami prawa (okres retencji danych).
2. W przypadku kiedy okresy retencji danych osobowych nie wynikają wyraźnie z przepisów prawa, Administrator określa te okresy samodzielnie, z uwzględnieniem uzasadnionych wskazań Administratora co do okresu przechowywania określonych danych osobowych. W przypadku gdy okres retencji danych osobowych wynika z przepisów prawa, ma on pierwszeństwo przed postanowieniami Polityki i jakichkolwiek Regulacji Wewnętrznych.
3. Administrator zapewnia, że w przypadku dezaktualizacji wszystkich celów przetwarzania danych osobowych, nie będą realizowane na nich jakiekolwiek operacje przetwarzania za wyjątkiem przygotowania do usunięcia i ich usunięcia (za równoznaczne z usunięciem uznaje się anonimizację danych).

§ 4.
Kryteria ustalenia terminu usunięcia danych osobowych

1. Aby określić termin usunięcia danych osobowych, należy:
   1) sprawdzić, czy ma zastosowanie szczególny przepis prawa, który wskazuje okres przechowywania danych osobowych przetwarzanych w ramach procesu. Załącznik nr 1 do niniejszej Polityki zawiera listę przykładowych przepisów i zakres ich zastosowania.
   2) określić, jaki zakres danych osobowych jest niezbędny do osiągnięcia danego celu przetwarzania.
   3) odpowiedzieć, kiedy dany cel przetwarzania zostaje osiągnięty lub przestaje być realizowany.
   4) ustalić czy przepis prawa szczególny wymaga dłuższego okresu przechowywania określonych danych osobowych (np. z powodu zapewnienia dokumentacji na cele postępowania podatkowego, do czasu przedawnienia zobowiązań podatkowych).
2. Postanowienia ust.1. należy zrealizować przy pomocy formularza, który stanowi Załącznik nr 2 do niniejszej Polityki. Określając okresy retencji uwzględnia się w szczególności:
   1) obowiązki prawne ciążące na Administratorze w zakresie przechowywania określonych danych osobowych lub dokumentów zawierających dane osobowe (np. akta osobowe pracowników, akta studenta, dokumenty związane ze statystyką),
   2) potencjalną niezbędność przetwarzania danych osobowych dla celów związanych z ustalaniem, dochodzeniem lub obroną przed potencjalnymi roszczeniami i związanymi z tym okresami przedawnienia roszczeń, wynikających z Kodeksu Cywilnego,
   3) niezbędność ich przetwarzania z uwagi na realizacje celu, dla którego zostały pozyskane.
3. Przed usunięciem danych osobowych należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji danych, w szczególności poprzez sprawdzenie czy:
   1) nie występuje obowiązek prawny ciążący na Administratorze,
   2) nie nastąpiło przerwanie lub zawieszenie okresu przedawniania roszczeń, skutkujące koniecznością dalszego przetwarzania danych osobowych,
   3) dalsze przechowywanie nie jest konieczne w związku z biegnącym okresem przedawnienia zobowiązań podatkowych.
4. Usunięcie powinno nastąpić niezwłocznie po upływie terminu określonego zgodnie z ust. 1. z uwzględnieniem okresu koniecznego do podjęcia niezbędnych czynności technicznych i organizacyjnych związanych z usunięciem danych osobowych.
5. Terminem usunięcia danych osobowych jest pierwszy dzień, kiedy przetwarzane dane osobowe nie są już niezbędne do celów, w których są przetwarzane. Dane osobowe nie są już niezbędne do celów, w których są przetwarzane, gdy:

1) upłynie okres ich przechowywania wskazany przez szczególny przepis prawa (np. upływ okresów przedawnienia roszczeń),
2) cel przetwarzania zostaje osiągnięty, lub
3) Uczelnia nie dąży już do celu, w którym te dane osobowe są przetwarzane.

6. Za usuwanie dokumentacji papierowej i elektronicznej odpowiadają Kierownicy komórek organizacyjnych Uczelni, Dyrektor Biblioteki oraz Dziekani.
7. Okresy retencji określone w RCP (Rejestr Czynności Przetwarzania) oraz w Załączniku nr 2 do niniejszej Polityki mogą ulegać zmianie w związku ze zmianą obowiązujących przepisów prawa. W takim wypadku należy zaktualizować RCP oraz Załącznik nr 2 do Polityki.

ZAŁĄCZNIKI

Załącznik 1 Przykładowe terminy usunięcia danych osobowych
Załącznik 2 Formularz oceny terminu usunięcia danych osobowych

PRZYKŁADY OKRESÓW RETENCJI DANYCH OSOBOWYCH

L.P.	CEL PRZETWARZANIA DANYCH/RODZAJ DOKUMENTÓW	PODSTAWA PRAWNA	OKRES PRZECHOWYWANIA
	1. SPRAWY PRACOWNICZE		
1.	REKRUTACJA Aplikacje składane przez Kandydatów (CV, listy motywacyjne, dokumenty potwierdzające uprawnienia i kwalifikacje, treść email, w którym przesłano aplikację, zapisy w systemie IT wykorzystywanym do rekrutacji).	Brak podstawy prawnej (wskazówki UODO).	Dokumenty i zapisy w systemie usuwane są niezwłocznie po zakończeniu rekrutacji, w związku z którą została przesłana aplikacja kandydata, nie później niż po upływie 1 miesiąca.
2.	BAZA POTENCJALNYCH KANDYTATÓW Prowadzenie bazy danych potencjalnych kandydatów na potrzeby przyszłych rekrutacji (CV, listy motywacyjne, dokumenty potwierdzające uprawnienia i kwalifikacje, treść email, w którym przesłano aplikację, zapisy w systemie IT wykorzystywanym do rekrutacji).	Brak podstawy prawnej (wskazówki UODO).	Dokumenty i zapisy w systemie usuwane są niezwłocznie po cofnięciu zgody na przetwarzanie danych osobowych na potrzeby przyszłych rekrutacji nie później niż po upływie 12 miesięcy od zakończenia postępowania rekrutacyjnego lub otrzymania aplikacji (jeżeli nie była prowadzona rekrutacja).
3.	WYKONYWANIE UMOWY O PRACĘ Dokumentacja w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników, w tym skrócone listy płac, wykaz nadgodzin, premie uznaniowe, paski do wypłaty, zajęcia komornicze, szkolenia pracowników.	Ustawa o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych Art. 125a; ustawa o narodowym zasobie archiwalnym i archiwach (Art. 51u w zw. z § 6 rozporządzenia MPiPS ws. zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika).	Dokumenty przechowywane są przez okres 50 lat od dnia zakończenia przez pracownika pracy. UWAGA ZMIANY OD 1.01.2019 R. Skrócenie okresu przechowywania dokumentacji obejmie wszystkich pracowników zatrudnionych po dniu wejścia w życie ustawy, tj. po dniu 1 stycznia 2019 r. Z 50 NA 10 LAT Dla pracowników zatrudnionych w okresie po dniu 31 grudnia 1998 r. a przed dniem 1 stycznia 2019 r. zasadą będzie przechowywanie dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracownika przez okres 50 lat od dnia rozwiązania lub wygaśnięcia stosunku pracy, chyba że pracodawca złoży oświadczenie o zamiarze przekazania za wszystkich zatrudnionych w tym okresie pracowników i zleceniobiorców raportów informacyjnych oraz raporty te faktycznie złoży. Pracodawca będzie więc mógł również skrócić do 10 lat okres przechowywania dokumentacji obecnych lub byłych pracowników, którzy zostali zatrudnieni po 1998 r. a przed 1 stycznia 2019 r., jeśli złoży w ZUS raport informacyjny, w którym znajdą się informacje niezbędne do wyliczenia emerytury lub renty danego pracownika (może ale nie musi).
4.	INFORMACJA O KARZE	art. 113 kodeks pracy	po roku nienagannej pracy usuwa się odpis zawiadomienia o karze
5.	WYKONYWANIE UMOWY O PRACĘ Dokumentacja związana z oceną pracowniczą,	art. 291 kodeksu pracy	Dokumenty przechowywane przez okres 3 lat od dnia zakończenia stosunku pracy (za wyjątkiem dokumentów, których konieczność dłuższego

	Dokumentacja wytworzona w związku z utrzymywaniem ZFŚS Umowy dotyczące dofinansowania szkoleń i inne umowy cywilnoprawne z pracownikami, Dokumentacja związana z obsługą świadczeń dodatkowych (karty sportowe, medyczne, ubezpieczenie grupowe) Dokumentacja związana z powierzeniem mienia pracownikom (urządzenia mobilne, samochód)		przechowywania wynika z właściwych przepisów prawa przede wszystkim w zakresie rachunkowości i podatkowych oraz przypadków gdy przechowywanie jest niezbędne z uwagi na bieg przedawnienia roszczeń pracownika lub zobowiązań podatkowych)
6.	WYKONYWANIE UMOWY z współpracownikami CV, listy motywacyjne, dokumenty potwierdzające uprawnienia i kwalifikacje, treść email, w którym przesłano aplikację, Umowa o współpracy (zlecenie dzieło itp.) Dokumentacja związana z oceną współpracownika, Umowy dotyczące dofinansowania szkoleń i inne umowy cywilnoprawne z współpracownikiem, Dokumentacja związana z obsługą świadczeń dodatkowych (karty sportowe, medyczne, ubezpieczenie grupowe) Dokumentacja związana z powierzeniem mienia (urządzenia mobilne, samochód)	Art. 118 kodeksu cywilnego, Art. 646 kodeksu cywilnego Art. 751 kodeksu cywilnego	Dokumenty przechowywane przez okres Od 2019 r. – przez 10 lat – na potrzeby ZUS, dowody potwierdzające pracę na podstawie umowy zlecenia przez okres 10 lat. - 3 lat (umowa zlecenia, świadczenia usług) pozostałe dane związane z umową zlecenia albo - 2 lat (umowa o dzieło) od dnia zakończenia współpracy (za wyjątkiem dokumentów, których konieczność dłuższego przechowywania wynika z właściwych przepisów prawa przede wszystkim w zakresie rachunkowości i podatkowych oraz przypadków gdy przechowywanie jest niezbędne z uwagi na bieg przedawnienia roszczeń pracownika lub zobowiązań podatkowych) Art. 118 kodeksu cywilnego Terminy przedawnienia roszczeń Jeżeli przepis szczególny nie stanowi inaczej, termin przedawnienia wynosi sześć lat, a dla roszczeń o świadczenia okresowe oraz roszczeń związanych z prowadzeniem działalności gospodarczej – trzy lata. Jednakże koniec terminu przedawnienia przypada na ostatni dzień roku kalendarzowego, chyba że termin przedawnienia jest krótszy niż dwa lata.
7.	OBSŁUGA WYPADKÓW PRZY PRACY (protokoły, wykazy, dokumenty związane z wypadkiem)	Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalania okoliczności i przyczyn wypadków przy pracy (Dz. U. Nr 105, poz. 870) art. 234 § 3(1) kodeksu pracy	10 lat od dnia wypadku przy pracy
8.	Rejestr pracowników narażonych na działanie substancji chemicznych, ich mieszanin, czynników lub procesów technologicznych o działaniu rakotwórczym lub mutagennym.	Rozporządzenia MZ z dnia 24 lipca 2012 r. ws. substancji chemicznych, ich mieszanin, czynników lub procesów technologicznych o działaniu rakotwórczym lub mutagennym w środowisku pracy (§ 5 ust. 1).	40 lat po ustaniu narażenia
9.	Rejestr pracowników narażonych na działanie szkodliwych czynników biologicznych zakwalifikowanych do grupy 3 lub 4 zagrożenia.	Rozporządzenie MPiPS ws. szkodliwych czynników biologicznych dla zdrowia w środowisku pracy oraz ochrony zdrowia pracowników zawodowo narażonych na te czynniki.	10 lat od dnia ustania narażania. **Wyjątek:** W przypadku narażenia na szkodliwy czynnik biologiczny, który może być przyczyną choroby: Rozporządzenie MPiPS ws. szkodliwych czynników biologicznych dla zdrowia w środowisku pracy oraz ochrony zdrowia pracowników zawodowo narażonych na te czynniki. 1) przewlekłej lub utajonej,

			2) która, w świetle obecnej wiedzy, jest niemożliwa do zdiagnozowania do czasu rozwinięcia się choroby, 3) o wyjątkowo długim okresie wylęgania, 4) o nawracającym charakterze w długim okresie pomimo leczenia, 5) mogącej powodować poważne, długookresowe powikłania - rejestr przechowywany jest przez okres 40 lat od dnia ostatniego odnotowanego przypadku narażenia.
10.	Rozporządzenie MZ z dnia 29 lipca 2010 r. ws. rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów.	Dokumentacja medyczna służby medycyny pracy.	20 lat od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, a w odniesieniu do pracowników zawodowo narażonych na czynniki rakotwórcze, mutagenne oraz biologiczne 3 lub 4 grupy zagrożenia, które mogą być przyczyną choroby, 40 lat po ustaniu narażenia.
	2. DOKUMENTY PODATKOWE		
11.	Ewidencje prowadzone dla celów podatkowych; podatkowe księgi przychodów i rozchodów, a także inne, rejestry i inne związane z nimi dokumenty; kopie i oryginały faktur VAT, dokumenty związane z poborem i inkasem podatkowym, księgi podatkowe i związane z ich prowadzeniem dokumenty, pozostała dokumentacja podatkowa.	Ordynacja podatkowa (art. 86 § 1 i art. 70 § 1), ustawa o podatku dochodowym od osób fizycznych (art. 24a i art. 25a), ustawa o podatku dochodowym od osób prawnych (art. 9 i art. 9a), art. 109 i art. 111 ustawy o podatku od towarów i usług.	Dokumentację podatkową należy przechowywać **przez okres 5 lat**, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku.
	3. DOKUMENTY RACHUNKOWE		
12.	• **księgi rachunkowe** – 5 lat, • **dowody księgowe dotyczące wpływów ze sprzedaży detalicznej** – do dnia zatwierdzenia sprawozdania finansowego za dany rok obrotowy, nie krócej jednak niż do dnia rozliczenia osób, którym powierzono składniki majątku objęte sprzedażą detaliczną, • **dowody księgowe dotyczące wieloletnich inwestycji** rozpoczętych, pożyczek, kredytów oraz umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętym postępowaniem karnym albo podatkowym	Ustawa o rachunkowości (art. 74).	Okres przechowywania dokumentów rachunkowych oblicza się od początku roku następującego po roku obrotowym, którego dane zbiory dotyczą.

	– **przez 5 lat** od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione, • **dokumentację przyjętego sposobu prowadzenia rachunkowości** – przez okres jej ważności i dodatkowo przez 3 lata po tym okresie, • **dokumenty inwentaryzacyjne** – 5 lat, • **pozostałe dowody księgowe i dokumenty** – 5 lat.		
	4. DOKUMENTY ZUS		
13.	**Dokumenty zgłoszeniowe** **Dokumenty rozliczeniowe** **Dokumenty płatnicze**	Ustawa o systemie ubezpieczeń społecznych (art. 36).	a) dokumenty zgłoszeniowe – aż do zakończenia prowadzenia działalności, b) kopie dokumentacji rozliczeniowych i imiennych raportów miesięcznych oraz dokumentów je korygujących należy przechowywać **przez okres 5 lat od dnia przekazania ich do ZUS w formie elektronicznej lub papierowej**.
14.	Dokumenty konieczne do udowodnienia uprawnień do świadczeń z ubezpieczenia emerytalnego i rentowego (m.in. zaświadczenia w celu udowodnienia okresów składkowych i nieskładkowych)	Ustawa o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Art. 125a).	50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika

15.	Kopie deklaracji rozliczeniowych i imiennych raportów miesięcznych oraz dokumentów korygujących	Ustawa o systemie ubezpieczeń społecznych (Art. 47).	5 lat od dnia ich przekazania do wskazanej jednostki organizacyjnej ZUS.
	5. PROCESY SĄDOWE, EWIDENCJE I MONITORING		
16.	Prowadzenie sporów sądowych Każdy rodzaj dokumentu związany z postępowaniem (pisma, orzeczenia, dowody	Kodeks Cywilny	6 lat, chyba że w tym czasie wszczęto egzekucję, która przerwała bieg przedawnienia art. 125 KC Roszczenie stwierdzone prawomocnym orzeczeniem sądu lub innego organu powołanego do rozpoznawania spraw danego rodzaju albo orzeczeniem sądu polubownego, jak również roszczenie stwierdzone ugodą zawartą przed sądem albo sądem polubownym albo ugodą zawartą przed mediatorem i zatwierdzoną przez sąd, przedawnia się z upływem sześciu lat. Jeżeli stwierdzone w ten sposób roszczenie obejmuje świadczenia okresowe, roszczenie o świadczenie okresowe należne w przyszłości przedawnia się z upływem trzech lat.
17.	Obsługa monitoringu wizyjnego Nagrania z monitoringu	Brak przepisu prawa	14 dni od dnia nagrania
18.	Obsługa korespondencji (rejestry poczty wychodzącej i przychodzącej)	Brak przepisu prawa	Maksymalnie 6 lat od dnia dokonania wpisu w rejestrze (potencjalny maksymalny okres przedawnienia roszczeń art. 118 KC)
	6. UMOWY		
19.	Wszelkiego rodzaju umowy, w szczególności zawierane z klientami i kontrahentami.	Tytuł VI Przedawnienie Roszczeń (Kodeks cywilny).	Umowy należy przechowywać do upływu okresu przedawnienia roszczeń wynikających z zawartej umowy: - co do zasady termin przedawnienia wynosi 6 lat* Art. 118. Terminy przedawnienia roszczeń termin przedawnienia wynosi 6 - sześć lat*, dla roszczeń o świadczenia okresowe oraz roszczeń związanych z prowadzeniem działalności gospodarczej – 3 trzy lata*.

			Jednakże koniec terminu przedawnienia przypada na ostatni dzień roku kalendarzowego, chyba że termin przedawnienia jest krótszy niż dwa lata. *Jeżeli przepisy szczególne nie stanowią inaczej.
	7. KONFERENCJE, KONKURSY		
	Dokumentacja dotycząca konferencji (programy, plany, wnioski, referaty, kosztorysy , itd.)	Brak podstawy prawnej (wytyczne Naczelnej Dyrekcji Archiwum Państwowego)	Przechowywanie wieczyste.
	8. NEWSLETTER		
20.	Dane przetwarzane w związku z zamówieniem usługi Newsletter, w szczególności adres e-mail.	Ustawa o świadczeniu usług drogą elektroniczną.	Dane zamawiającego Newsletter powinny być usuwane **niezwłocznie** na wyraźne żądanie osoby, której dane dotyczą.
	9. DANE ZWIĄZANE Z REKRUTACJĄ NA STUDIA		
21.	Dokumenty rekrutacyjne osób nieprzyjętych na studia (kwestionariusz osobowy, ksero świadectwa dojrzałości, ksero dyplomu, ksero suplementu, ksero wypisu z indeksu, ksero dowodu osobistego, dowód wniesienia opłaty rekrutacyjnej, itd.)	Brak przepisu prawa	Dokumenty należy przechowywać do upływu okresu przedawnienia roszczeń. Maksymalnie 6 lat od dnia zakończenia rekrutacji.
	10. DANE STUDENTÓW		
22.	Teczki akt osobowych studentów	§ 15 ust. 4 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r w sprawie studiów	Dokumenty należy przechowywać przez okres 50 lat w archiwum Uczelni.

FORMULARZ USTALANIA TERMINU USUNIĘCIA DANYCH OSOBOWYCH W PAŃSTWOWEJ WYŻSZEJ SZKOLE ZAWODOWEJ IM. WITELONA W LEGNICY	
Pytanie	**Odpowiedź**
JAKI JEST CEL PRZETWARZANIA DANYCH OSOBOWYCH?	
DANE O PROCESIE PRZETWARZANIA LUB DANE O KONKRETNYM REKORDZIE	
CZY I W JAKIM ZAKRESIE MA ZASTOSOWANIE SZCZEGÓLNY PRZEPIS PRAWA, KTÓRY WSKAZUJE OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH PRZETWARZANYCH W RAMACH PROCESU?	
JAKI JEST MINIMALNY OKRES PRZETWARZANIA DANYCH OSOBOWYCH NIEZBĘDNY DO OSIĄGNIĘCIA CELU PRZETWARZANIA?	
KIEDY DANY CEL PRZETWARZANIA ZOSTAJE OSIĄGNIĘTY LUB PRZESTAJE BYĆ REALIZOWANY?	
DLACZEGO WYŻEJ WYMIENIONY OKRES PRZETWARZANIA DANYCH OSOBOWYCH JEST NIEZBĘDNY DO OSIĄGNIĘCIA CELU PRZETWARZANIA?	
CZY, A JEŻELI TAK UCZELNIA COŚ STRACI USUWAJĄC TE DANE?	
CZY UWZGLĘDNIONO WSZYSTKIE ASPEKTY związane z OKRESEM PRZETWARZANIA? Np. przerwanie biegu przedawnienia/zmiany przepisów prawa	

Imię i nazwisko autora oraz data sporządzenia dokumentu: .....

Procedura udostępniania oraz powierzania przetwarzania danych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy

§ 1.
Cel procedury.

1. Niniejsza procedura jest elementem Polityki Ochrony Danych Osobowych.
2. Celem niniejszej procedury jest zapewnienie doboru podmiotów przetwarzających dane osobowe na zlecenie Administratora zgodnie z postanowieniami RODO, tj. w sposób który zapewnia zapewnienie przez podmiot przetwarzający wystarczających gwarancji wdrożenia odpowiednich środków technicznych, organizacyjnych, aby powierzone przez Administratora przetwarzanie danych osobowych spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.

§ 2.
Zakres stosowania oraz odpowiedzialność.

1. Niniejsza procedura sosowana jest w każdym przypadku zawierania przez Uczelnię umowy, porozumienia (w formie pisemnej, ustnej i każdej innej) z podmiotem trzecim w wyniku wykonania której Uczelnia a udostępnia dane swoich kontrahentów, pracowników lub innych osób, których dane dotyczą i ma zastosowanie do wyboru i oceny podmiotu przetwarzającego.
2. Działania opisane w niniejszej procedurze obowiązują, we wszystkich komórkach organizacyjnych Uczelni.
3. Odpowiedzialność za prawidłowy dobór podmiotu przetwarzającego ponosi osoba zawierająca w imieniu Administratora umowę lub osoba koordynująca przygotowanie umowy, porozumienia (w formie pisemnej, ustnej i każdej innej) z podmiotem trzecim, w wyniku wykonania której Uczelnia udostępnia dane swoich studentów, pracowników lub innych osób, których dane dotyczą.

§ 3.
Dobór podmiotu przetwarzającego

1. Powierzenie przetwarzania danych osobowych oznacza powierzenie w imieniu Uczelni przetwarzania danych osobowych podmiotowi spoza struktury organizacyjnej Uczelni (podmiot inny niż Uczelnia) w celach ustalanych przez Uczelnię.
2. Przed dokonaniem zakupu (w szczególności licencji na oprogramowanie, miejsca na serwerach) albo zawarciem każdej umowy, w szczególności związanej ze zlecaniem na zewnątrz określonych usług, zakupieniem usług, należy zbadać, czy w ramach wykonania takiej umowy Uczelnia powierza przetwarzanie danych osobowych, których jest administratorem - drugiej stronie umowy.
3. Uczelnia może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej (w tym zawartej elektronicznie), zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO. Umowa powierzenia przetwarzania powinna zawierać wszystkie elementy wymienione w art. 28 ust. 3 RODO. Wzór takiej umowy stanowi Załącznik nr 1 do niniejszej Polityki.
4. Potrzebę zawarcia lub aktualizacji umowy powierzenia przetwarzania zgłasza się bezpośrednio przełożonemu, załączając opinię osoby co do zakresu powierzonych danych, która będzie odpowiedzialna za organizację, projektowanie, zarządzanie zmianami oraz ustawiczne doskonalenie planowanego procesu przetwarzania danych osobowych.
5. Oceniając potrzebę zawarcia lub aktualizacji umowy powierzenia przetwarzania, osoba wskazana w ust. 4. określa przynajmniej:
    1) cel powierzenia przetwarzania,
    2) zakres danych osobowych, które mają być powierzane,
    3) kategorie osób, których dotyczą dane, które mają być powierzane,
    4) sugerowany podmiot lub podmioty przetwarzające,
    5) informacje świadczące o odpowiedniej wiedzy fachowej, wiarygodności i zasobach sugerowanego podmiotu lub podmiotów przetwarzających.
6. Przed powierzeniem przetwarzania danych osobowych Uczelnia w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych. Podmiot, któremu powierzono przetwarzanie danych obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przetwarzanie danych, o których mowa w RODO.
7. Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
8. W razie zawarcia umowy powierzenia przetwarzania, należy dokonywać regularnej oceny podmiotu przetwarzającego, a w szczególności w toku audytu systemu ochrony danych osobowych. Do oceny podmiotu przetwarzającego służy Załącznik nr 2, który można wypełnić samodzielnie lub przesłać do wypełnienia podmiotowi przetwarzającemu.
9. W sytuacji przekazywania danych osobowych do podmiotu znajdującego się w państwie trzecim (poza Europejskim Obszarem Gospodarczym) należy taką sytuację skonsultować z IOD.

10. Minimalne gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych przez podmiot przetwarzający opisuje Załącznik nr 3 do niniejszej Procedury.
11. IOD prowadzi rejestr zawartych umów powierzenia zgodnie z Załącznikiem nr 4.

§ 4.
Udostępnianie danych

1. Osoby, które udostępniają w imieniu Uczelni dane osobowe do podmiotu zewnętrznego (w formie papierowej lub elektronicznej), przed ich udostępnieniem mają obowiązek sprawdzić czy istnieją podstawy prawne umożliwiające wykonanie tych czynność, w tym:
    1) wymóg prawa dotyczący udostępnienia danych;
    2) zgoda osoby na udostępnienie danych innemu podmiotowi;
    3) zapis w umowie z podmiotem współpracującym, przy spełnieniu warunku, że udostępnienie nie narusza praw i wolności osoby, której dane dotyczą;
    4) wniosek o udostępnienie danych od podmiotu uprawnionego, ze wskazaniem podstawy prawnej do otrzymywania danego rodzaju danych osobowych.
2. Każda sytuacja dotycząca udostępnienia danych osobowych musi być konsultowana z IOD.
3. Dane osobowe udostępnia się odbiorcy danych na pisemny wniosek ze wskazaniem przez odbiorcę podstawy prawnej legalizującej przetwarzanie danych.
4 IOD odnotowuje zdarzenia udostępnienia w rejestrze odbiorców danych osobowych. W rejestrze odnotowywane są między innymi: imię i nazwisko lub nazwa odbiorcy, adres odbiorcy, podstawa prawna udostępnienia, data udostępnienia oraz zakres udostępnienia. Dopuszcza się załączanie do rejestru wydruku/kopii papierowej przekazanego zbioru danych.
5. W sytuacji kiedy system informatyczny umożliwia odnotowywanie informacji o odbiorcach danych, możliwe jest prowadzenie rejestru elektronicznego.
6. Na żądanie osoby, której dane zostały udostępnione odbiorcy danych, IOD udostępnia właściwe informacje na podstawie prowadzonego rejestru lub wygenerowanego raportu w systemie informatycznym, jeśli program udostępnia funkcjonalność rejestracji odbiorców danych.

ZAŁĄCZNIKI

ZAŁĄCZNIK 1 Umowa powierzenia przetwarzania danych osobowych
ZAŁĄCZNIK 2 Ankieta oceny umowy powierzenia przetwarzania danych osobowych oraz oceny działania podmiotu przetwarzającego
ZAŁĄCZNIK 3 Minimalne gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych
ZAŁĄCZNIK 4 Rejestr zawartych umów powierzenia

Załącznik nr 1 do
procedury powierzania i udostępniania danych

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... r. pomiędzy:

Państwową Wyższą Szkołą Zawodową im. Witelona w Legnicy, z siedzibą w Legnicy, ul. Sejmowa 5a, NIP 691-19-94-675, REGON 390624793,

reprezentowaną przez:

Rektora - Prof. dr hab. inż. Ryszarda K. Pisarskiego

zwaną dalej **„Administratorem"**

a

.....

reprezentowaną przez:

.....

zwanym dalej **„Podmiotem przetwarzającym",**

zaś wspólnie **„Stronami"**

W związku z zawarciem w dniu ..... r. Umowy zlecenia zwanej dalej „Umową główną", której przedmiotem są czynności związane z .....
Strony postanawiają, co następuje:

§ 1.
Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 *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 (zwane dalej „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu do przetwarzania.
3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający w celu .....
4. 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.
5. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.
6. Podmiot przetwarzający oświadcza, że przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

§ 2.
Zakres i cel przetwarzania danych

1. Dane osobowe dotyczą następujących kategorii osób: .....
2. Podmiot przetwarzający będzie przetwarzać, powierzone na podstawie Umowy głównej dane w następującym zakresie: .....
3. Administrator oświadcza, że charakter danych osobowych, powierzanych Umową główną, nie obejmuje szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 Rozporządzenia.
4. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy głównej z dnia ..... r.

§ 3.
Sposób wykonania umowy w zakresie przetwarzania danych osobowych

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 wart. 32 Rozporządzenia.
2. Wdrażając środki organizacyjne i techniczne, o których mowa powyżej, Podmiot przetwarzający:
   1) przestrzega wytycznych Administratora w zakresie sposobu zabezpieczenia procesów przetwarzania danych osobowych zgodnie z przepisami Rozporządzenia oraz innymi obowiązującymi przepisami prawa. Minimalne gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych wymaganych przez Administratora stanowi załącznik nr 1 do Umowy;
   2) powinien uwzględnić stan wiedzy technicznej oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których dane osobowe będzie przetwarzał na podstawie Umowy.
3. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
4. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, których dostęp jest niezbędny do wykonania usług określonych w Umowie głównej, w związku z którą przetwarzane są dane osobowe.
5. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 lit. b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy głównej, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
6. Podmiot przetwarzający biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.
7. Podmiot przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia.
8. Podmiot przetwarzający po zakończeniu realizacji Umowy głównej niezwłocznie, jednak nie później niż w ciągu 10 dni, zwraca powierzone dane Administratorowi oraz trwale usuwa wszelkie ich istniejące kopie.
9. Podmiot przetwarzający ma obowiązek powiadomić Administratora za pośrednictwem poczty elektronicznej, w przypadku stwierdzenia nieprawidłowości w terminie 48 godzin od wystąpienia zdarzenia o wszelkich incydentach dotyczących przetwarzania powierzonych danych osobowych, w tym przypadkowego lub nieupoważnionego dostępu do powierzonych danych osobowych, przypadkach utraty, zmiany powierzonych danych.
10. Zgłoszenie, o którym mowa w ust. 9 musi co najmniej:
    1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
11. Podmiot przetwarzający jest obowiązany do dokumentowania wszelkich okoliczności i zebrania wszelkich dowodów, które pomogą Administratorowi wyjaśnić szczegóły naruszenia, w tym jego charakter, skalę, skutki, czas zdarzenia, osoby odpowiedzialne oraz osoby poszkodowane.
12. Podmiot przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z niniejszą Umową przetwarzania danych.
13. Odpowiedzialność, o której mowa w ust. 11 obejmuje rzeczywiste szkody za niewykonanie, bądź nienależyte wykonanie niniejszej Umowy, będące następstwem okoliczności, za które Podmiot przetwarzający ponosi odpowiedzialność.

14. W przypadku, gdy osoba trzecia skieruje przeciwko Administratorowi roszczenia oparte na zarzucie niezgodnego z niniejszą Umową lub przepisami przetwarzania danych osobowych przez Podmiot przetwarzający, Strony ustalają poniższe zasady postępowania:
    1) Administrator zobowiązany jest niezwłocznie, nie później niż w terminie 3 dni roboczych od powzięcia wiedzy w tym przedmiocie – powiadomić Podmiot przetwarzający i wezwać go do udziału w wyjaśnieniu sprawy,
    2) Podmiot przetwarzający będzie brał czynny udział w wyjaśnieniu sprawy, w celu naprawienia powstałej szkody lub polubownego załatwienia sprawy w drodze negocjacji,
    3) w przypadku, gdy Strony wspólnie z osobą trzecią dojdą do porozumienia, że roszczenie osoby trzeciej jest uzasadnione i uzgodnią sposób zadośćuczynienia, Podmiot przetwarzający będzie zobowiązany do pokrycia roszczeń osoby trzeciej, chyba że naruszenie powstało z winy Administratora, wtedy do pokrycia roszczeń zobowiązany będzie Administrator,
    4) w razie braku porozumienia, o którym mowa w lit. c i wystąpieniem osoby trzeciej na drogę postepowania sądowego, Administrator niezwłocznie jednak nie później niż w terminie 7 dni od powzięcia takiej wiadomości powiadomi Podmiot przetwarzający,
    5) po rozpoczęciu postępowania sądowego Podmiot przetwarzający będzie w nim uczestniczył jako interwenient uboczny, po stronie pozwanej bądź w miejsce strony pozwanej, udzieli wszelkiej pomocy w celu obrony przed roszczeniami osoby trzeciej, w szczególności w zakresie dostarczenia informacji i dokumentów, w których jest w posiadaniu a związanych z dochodzonym roszczeniem.
    6) w przypadku zawarcia ugody, Podmiot przetwarzający zwolni Administratora z obowiązku naprawienia szkody w takim zakresie w jakim wynika to z ugody.
15. Administrator odpowiada za szkody, jakie powstaną u Podmiotu przetwarzającego lub osób trzecich w wyniku przetwarzania danych niezgodnego z niniejszą umową, postanowieniami Rozporządzenia lub innych ogólnie obowiązujących przepisów prawa, o ile wynikają one z winy Administratora.

§ 4.
Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej Umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3-dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybienia stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. Podmiot przetwarzający umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
6. Administrator ma prawo dokonywać regularnej oceny Podmiotu przetwarzającego, za pomocą formularza stanowiącego załącznik nr 2 do Umowy.
7. W związku z obowiązkiem określonym w ust. 4 Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów powszechnie obowiązujących o ochronie danych.

§ 5.
Podpowierzenie

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umowa do dalszego przetwarzania osobie trzeciej jedynie w celu wykonania umowy po uzyskaniu uprzedniej zgody Administratora.
2. Podmiot przetwarzający zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, a także zapewniało ochronę praw osób, których dane dotyczą.
3. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podwykonawca winien zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6.
Czas obowiązywania umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania umowy głównej, o której mowa w § 2 ust. 4 oraz po zakończeniu realizacji tej umowy – do dnia realizacji § 3 ust. 7.
2. Wszelkie zmiany niniejszej Umowy i jej warunków mogą być dokonywane za zgodą obu Stron wyrażoną na piśmie pod rygorem nieważności.

3. Treść Umowy może być zmieniana m.in. w przypadku zmiany przepisów prawa i konieczności dostosowania treści Umowy do tych przepisów lub zmiany regulacji wewnętrznych dotyczących przetwarzania danych osobowych obowiązujących u Administratora.

§ 7.
Rozwiązanie umowy

1. Każda ze stron może rozwiązać niniejszą Umowę w trybie natychmiastowym w przypadku, gdy druga Strona rażąco naruszy postanowienia niniejszej Umowy lub Umowy głównej, a w szczególności zasad dotyczących ochrony powierzonych danych osobowych.
2. W przypadku rozwiązania Umowy Podmiot przetwarzający zobowiązany jest niezwłocznie, jednak nie później niż w terminie 7 dni, zwrócić Administratorowi dane osobowe powierzone do przetwarzania oraz dokonać trwałego zniszczenia wszelkich kopii zawierających powierzone dane osobowe. Zwrot zostanie potwierdzony protokołem przekazania danych podpisanym przez obie Strony.

§ 8.
Zasady zachowania tajemnicy

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, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych, o których mowa w ust. 1, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy głównej, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy głównej.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych, o których mowa w ust. 1, gwarantowały zabezpieczenie danych w tym w szczegó1ności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§ 9.
Postanowienia końcowe

1. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, Rozporządzenia oraz inne przepisy prawa powszechnie obowiązującego.
2. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla siedziby Podmiotu przetwarzającego.
3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednej dla każdej ze Stron.

ADMINISTRATOR **PODMIOT PRZETWARZAJĄCY**

_____ _____

WERYFIKACJA/ANALIZA ŚRODKÓW ZABEZPIECZEŃ ORGANIZACYJNYCH i TECHNICZNYCH ZASTOSOWANYCH PRZEZ PODMIOT PRZETWAZRAJĄCY	
ADMINISTRATOR DANYCH	**Państwowa Wyższa Szkoła Zawodowa im. Witelona w Legnicy**
PODMIOT PRZETWARZAJĄCY	

Grupa zabezpieczeń	**Opis zabezpieczeń**	Uzupełnia Przetwarzający:
Środki organizacyjne	1. Zapewniono kontrolę nad dostępem do Danych osobowych, w szczególności poprzez:	
	1) wyznaczenie osób upoważnionych do przetwarzania danych osobowych na polecenie Administratora i wydanie imiennych upoważnień do przetwarzania danych osobowych,	
	2) zapewnienie, że osoby posiadające upoważnienia, o których mowa w pkt 1 zobowiązały się do zachowania tajemnicy.	
	2. Zapewniono szkolenia z zakresu bezpieczeństwa przetwarzania danych osobowych dla osób biorących udział w procesie przetwarzania.	
	3. Przyjęto i wdrożono polityki ochrony danych, w tym polityki bezpieczeństwa danych w systemach informatycznych.	
	4. Prowadzony jest rejestr kategorii czynności przetwarzania danych.	
	5. Przyjęto i wdrożono procedurę związaną z reagowaniem na naruszenia ochrony danych, w tym prowadzony jest rejestr naruszeń ochrony danych osobowych.	
	6. Prowadzona jest analiza ryzyka w zakresie przetwarzania danych osobowych.	
Środki ochrony fizycznej i środowiskowej stosowane w celu zabezpieczenia budynków oraz	1. Zapewniono kontrolę dostępu fizycznego do budynku oraz pomieszczeń, w których przetwarzane są dane osobowe.	
	2. Zabezpieczono miejsca przetwarzania danych osobowych od zdarzeń losowych (np. pożar, zalanie).	

pomieszczeń, w których przetwarzane są dane osobowe	3. Zapewniono ochronę danych osobowych przed dostępem osób postronnych, uszkodzeniem lub zniszczeniem przez nie.	
	4. Przyjęto i wdrożono procedurę niszczenia danych.	
Zabezpieczenia techniczne i systemów teleinformatycznych	1. Zapewniono bezpieczeństwo danych osobowych, w tym poufność danych poprzez:	
	1) stosowanie unikalnych identyfikatorów użytkowników,	
	2) stosowanie złożonych haseł dostępowych użytkowników (co najmniej 8 znaków, w tym przynajmniej 1 wielka litera, 1 mała litera, 1 cyfra lub znak specjalny),	
	3) stosowanie wymuszonej okresowej zmiany haseł użytkowników (nie rzadziej niż co 30 dni),	
	4) legalne i aktualne oprogramowanie, wspierane przez producenta, w tym oprogramowanie antywirusowe lub inne oprogramowanie identyfikujące podejrzane aktywności w systemach, na stacjach roboczych oraz serwerach mailowych, w szczególności filtrowanie poczty: antyspam, antywirus i anti-malware.	
	5) kontrola i nadzór ruchu w sieci wewnętrznej, tj. monitoring aktywności użytkowników, blokowanie zewnętrznych nośników.	
	6) kontrolę oraz monitorowanie styku sieci wewnętrznej z siecią Internet (zapory ogniowe, proxy),	
	7) środki kryptograficznej ochrony na poziomie transmisji danych przesyłanych z wykorzystaniem sieci Internet, tj. szyfrowanie informacji zawierających Dane osobowe wysyłanych lub udostępnianych elektronicznymi kanałami wymiany informacji,	
	8) przetwarzanie informacji zawierających dane osobowe na zabezpieczonych nośnikach w postaci szyfrowanych dysków urządzeń mobilnych, w tym przenośnych pamięci masowych,	

	10) mechanizmy identyfikacji i uwierzytelniania użytkowników (co najmniej identyfikator i hasło) w przypadku udostępniania aplikacji dostępnych przez sieć Internet.	
	2. Zapewniono bezpieczeństwo danych osobowych, w tym ich dostępność i odporność systemów poprzez:	
	1) sformalizowane zasady zgłaszania incydentów związanych z bezpieczeństwem systemów,	
	2) systemy wykonywania i przechowywania kopii zapasowych,	
	3) systemy podtrzymania napięcia (UPS),	
	4) ograniczanie pojedynczych punktów awarii lub minimalizowanie ryzyka związanego z wystąpieniem awarii,	
	3. Zapewniono bezpieczeństwo danych osobowych, w tym ich integralność i realizację zasady rozliczalności poprzez:	
	1) logowanie działalności użytkowników (repozytorium z logami),	
	2) logowanie wykonanych zmian na danych osobowych przez użytkowników,	
WYMAGANIA RODO	Czy podmiot przetwarzający spełnia wymagania RODO z art. 24 RODO?	
	Czy podmiot przetwarzający spełnia wymagania RODO z art. 32 RODO?	
	Czy podmiot przetwarzający spełnia wymagania RODO z art. 27 RODO?	

PODPIS OSOBY REPREZENTUJĄCEJ PROCESORA

_____

MINIMALNE GWARANCJE WDROŻENIA ODPOWIEDNICH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH PRZEZ ZLECENIOBIORCĘ

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

Administrator **Przetwarzający**

....

Załącznik nr 4 do Procedury udostępniania oraz powierzania danych

EWIDENCJA ZAWARTYCH UMÓW POWIERZENIA

L.p.	CZY UCZELNIA JEST ADO CZY PROCESOREM	DATA ZAWARCIA UMOWY	NAZWA PODMIOTU I DANE KONTAKTOWE	ZAKRES POWIERZONYCH DANYCH	PRZEDMIOT UMOWY PODSTAWOWEJ	DATA ZAKOŃCZENIA WSPÓŁPRACY
1						

REJESTR NARUSZEŃ DANYCH OSOBOWYCH

Nazwa ADO				
UCZELNIA:				
DANE IOD:				
Imię i nazwisko wypełniającego rejestr:				
Stanowisko wypełniającego rejestr:				

Data i godzina stwierdzenia naruszenia	Organ nadzoru CZY I KIEDY powiadomiono	Osoby, których dane osobowe zostały naruszone			Okoliczności i charakter naruszenia	Konsekwencje naruszenia	Zastosowane środki w celu zaradzenia naruszeniu ochrony danych osobowych	Proponowane środki w celu zaradzenia naruszeniu ochrony danych osobowych
		kategorie osób	ilość osób	ilość wpisów danych osobowych				

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. CEL INSTRUKCJI

1.1. Niniejsza instrukcja jest elementem Polityki Ochrony Danych Osobowych przyjętej przez Uczelnię.

1.2. Celem Instrukcji jest:

a) Zdefiniowanie przykładowego, typowego katalogu zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych.

b) Ustalenie sposobu reagowania na zagrożenia i incydenty.

c) uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych, wynikających z zaistnienia naruszeń lub zagrożeń bezpieczeństwa danych, oraz zagrożeń systemu ochrony danych osobowych.

d) zapewnienie zgodności działania Uczelni z RODO, w szczególności zapewnienia, że zdarzenia związane z naruszeniem bezpieczeństwa, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących i wypełnienie obowiązków Uczelni wynikających z RODO.

e) minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1.3. Niniejsza Instrukcja obejmuje w szczególności:

a) realizację obowiązku zgłaszania naruszenia ochrony danych osobowych, o którym mowa w art. 33 ust. 1 i 2 RODO,

b) realizację obowiązku zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 ust. 1 RODO),

c) wdrożenie środków planowanych w celu zaradzenia naruszeniu,

1.4. Instrukcja obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na prawa lub wolności osób fizycznych, zgodność z wymaganiami RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

1.5. Ilekroć mowa o:

a) naruszeniu ochrony danych osobowych - rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

b) incydencie - rozumie się przez to zdarzenie lub serię powiązanych ze sobą zdarzeń, które skutkują lub mogą skutkować naruszeniem ochrony danych osobowych,

c) osoba wyznaczona przez ADO – rozumie się Inspektora Ochrony Danych - IOD,

d) zagrożenie – potencjalna możliwość wystąpienia incydentu;

e) korekcja – działanie w celu wyeliminowania skutków incydentu;

f) działanie korygujące – jest to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

g) działania zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądane;

h) kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki bezpieczeństwa i instrukcji zarzadzania systemem informatycznym,

i) raport – raport, powiadomienie ustne lub na wzorze stanowiącym załącznik do Instrukcji.

j) IOD – oznacza wyznaczonego w ADO Inspektora Ochrony Danych,

k) PODO – Polityka Ochrony Danych Osobowych.

2. ZAKRES STOSOWANIA i ODPOWIEDZIALNOSĆ

2.1. Obowiązki i Działania opisane w niniejszej instrukcji obowiązują wszystkich pracowników Uczelni.

2.2. Osobą odpowiedzialną za nadzór nad realizacją procedury jest IOD.

2.3. Każdy pracownik Uczelni w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest:

a) bezzwłocznie powiadomić IOD w jeden z następujących sposobów:
- telefonicznie wew. 281
- email IOD@pwsz.legnica.edu.pl

b) podjąć rozsądne kroki zmierzające do usunięcia skutków naruszenia.

2.4. Za naruszanie ochrony danych osobowych obowiązują kary przewidziane przepisami prawa.

2.5. Za naruszenie ochrony danych osobowych ADO może stosować kary porządkowe, niezależnie od zastosowania kar, o których mowa w pkt. 2.4.

3. TYPOWE ZAGROŻENIA I INCYDENTY

3.1. Naruszenie ochrony danych osobowych dotyczy danych osobowych utrwalonych w formie fizycznych nośników danych (dokumentacja) jak i w formach elektronicznych (dane osobowe wprowadzone w systemie, plikach itp.).
3.2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3.3. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników utrata/zagubienie danych);
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. IDENTYFIKACJA NARUSZENIA I SPOSÓB REAGOWANIA NA NARUSZENIA

4.1. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych, osoba wyznaczona przez Uczelnię lub Uczelnię prowadzi postępowanie wyjaśniające, w toku którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki, zarówno dla Uczelni, jak i osób, których dane dotyczyły;
   b) podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w Uczelni,
   c) wskazuje osoby odpowiedzialne za wystąpienie sytuacji oraz ewentualnie inicjuje działania dyscyplinarne;
   d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   e) dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu z zagrożenia bezpieczeństwa danych osobowych , podejmuje działania zapobiegawcze.
   f) ustala czy należy dokonać zgłoszenia incydentu naruszenia bezpieczeństwa do PODO,
   g) ocenia, czy w związku z naruszeniem ochrony danych osobowych zachodzi wysokie ryzyko naruszenia praw i wolności osób fizycznych i czy należy powiadomić o tym podmiot danych.
4.2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych IOD prowadzi postępowanie wyjaśniające.
4.3. ADO na wniosek IOD może powołać zespół ds. naruszeń, w skład którego mogą wchodzić
   a) LADO,
   b) pracownik IT – wg. potrzeby,
   c) Radca Prawny,
   d) kierownik działu w którym stwierdzono naruszenie.
4.4. Obowiązki Zespołu ds. naruszeń:
   a) niezwłoczne reagowanie na incydenty w określony i z góry ustalony sposób;
   b) ocenę istniejących i potencjalnych zagrożeń w zakresie naruszenia ochrony danych osobowych;
   c) ocenę przyczyn i skutków incydentów naruszenia ochrony danych osobowych informacji w tym gromadzenie materiału dowodowego;
   d) przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem.
4.5. Pracami Zespołu ds. naruszeń kieruje IOD.
4.6. IOD lub Zespół ds. naruszeń prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   b) ustala konieczność powiadomienia organu nadzorczego oraz osoby, której dane dotyczą,
   c) inicjuje ewentualne działania dyscyplinarne,
   d) działa na rzecz przywrócenia działań Uczelni po wystąpieniu incydentu,
   e) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
4.7. Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu innych odpowiednich osób.
4.8. W przypadku powołania Zespołu ds. Naruszeń zbiera się on niezwłocznie.
4.9. IOD/Zespół ds. naruszeń dokumentuje okoliczności naruszenia w wybrany przez siebie sposób, z zachowaniem zasady rozliczalności np.:
   a) sporządza notatkę z przeprowadzonych oględzin miejsca zdarzenia,
   b) sporządza kopię obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem,

c) sporządza kopię zapisów rejestrów systemu informatycznego służącego do przetwarzania danych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu,
d) zbiera pisemne wyjaśnienia od osoby, która ujawniła naruszenie.

4.10. IOD dokumentuje czynności podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu (załącznik nr 2 lub 3 do instrukcji) o naruszeniu ochrony danych osobowych wg załączonego wzoru który zawiera co najmniej:
a) Powinno zawierać kod formy naruszenia danych osobowych wg załączonego katalogu zagrożeń i incydentów bezpieczeństwa danych osobowych (załącznik nr 1) (nie jest to obligatoryjne);
b) ustala datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, skutki, oraz wielkość szkód które zaistniały;
c) zabezpiecza ewentualne dowody winy;
d) ustala osoby odpowiedzialne za naruszenia;
e) sporządza dokumentację z naruszenia dla zachowania zasady rozliczalności wg RODO,
f) ustala czy należy dokonać zgłoszenia o naruszeniu do PUODO oraz dla podmiotu danych w terminie pozwalającym dokonać zgłoszenia naruszenia organowi nadzorczemu przez ADO (maksymalnie 72 godziny od stwierdzenia incydentu).
g) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
h) inicjuje działania dyscyplinarne;
i) rekomenduje działania prewencyjne (korekcyjne, korygujące, zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.

4.11.Zalecenia co do dokumentowania:
a) dla danych z dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony.
b) dla danych z systemów, dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).

4.12. IOD ewidencjonuje każdy Incydent w „Rejestrze incydentów" (załącznik nr 4 do niniejszej Instrukcji).

4.13.Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
a) zgłoszenia od kierowników komórek organizacyjnych Uczelni lub pracowników;
b) wyniki kontroli w tym ustalone przyczyny i okoliczności naruszenia bezpieczeństwa danych osobowych,
c) doniesienia podmiotów danych.

4.14. W przypadku, gdy IOD lub Zespół ds. Naruszeń stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
a) źródło powstania incydentu lub zagrożenia;
b) zakres działań korygujących lub zapobiegawczych;
c) termin realizacji, osobę odpowiedzialną.

i przedstawia rekomendacje do zatwierdzenia ADO lub LADO.

5. USTALENIE OBOWIĄZKU ZGŁASZANIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

5.1. IOD dokonuje analizy w celu określenia, czy wykryte naruszenie ochrony danych osobowych podlega obowiązkowi zgłoszenia organowi nadzorczemu oraz osobom, których dotyczą dane objęte naruszeniem. Aby dokonać tej analizy należy określić poziom ryzyka naruszenia praw lub wolności osób fizycznych, postępując zgodnie z pkt. 5.2. Tak ustalony poziom ryzyka należy wprowadzić i opisać w dokumentacji naruszenia ochrony danych.

5.2 Przy określaniu poziomu ryzyka naruszenia praw i wolności osoby, której dane dotyczą, odwołując się do poszczególnych kategorii potencjalnych naruszeń, należy każdorazowo:
a) wskazać źródła ryzyka,
b) sporządzić opis potencjalnej szkody,
c) oszacować wagę zagrożenia,
d) oszacować prawdopodobieństwo wystąpienia danej szkody,
e) obliczyć poziom ryzyka,
f) wydać rekomendacje.

Poniższa tabela zawiera opis kategorii potencjalnych naruszeń, jak również wyjaśnienie liter a)-f).

ZAGADNIENIE	WYJAŚNIENIE
Kategorie potencjalnych naruszeń	
Przetwarzanie nieprawidłowych lub niepełnych danych	Przetwarzanie danych nieprawidłowych w świetle celów ich przetwarzania stanowi naruszenie art. 5 ust. 1 lit. d RODO (obowiązek zapewnienia prawidłowości danych). W tej kategorii znajdują się też możliwe naruszenia prawa do sprostowania danych (art. 16 RODO).
Nieuprawniony dostęp	W razie uzyskania dostępu do danych przez osoby nieuprawnione, naruszona zostałaby zasada integralności i poufności danych (art. 5 ust. 1 lit. f RODO) oraz obowiązek przetwarzania danych wyłącznie na polecenie administratora (art. 29 RODO).
Nieuprawnione ujawnienie lub udostępnienie	Chodzi o upublicznienie lub udostępnienie danych osobowych bez podstawy prawnej. Stanowiłoby to naruszenie zasady ograniczenia celu (art. 5 ust. 1 lit. b RODO) oraz zakazu przetwarzania danych osobowych bez podstawy prawnej (art. 6, 9 lub 10 RODO, w zależności od kategorii danych, które są przetwarzane).
Przypadkowe lub nieuprawnione zniszczenie, utrata lub uszkodzenie danych	W razie przypadkowego lub nieuprawnionego zniszczenia, utraty lub uszkodzenia danych, doszłoby do naruszenia zasady integralności i poufności danych (art. 5 ust. 1 lit. f RODO).
Nieuprawniona modyfikacja	W razie nieuprawnionej modyfikacji danych, doszłoby do naruszenia zasady prawidłowości danych (art. 5 ust. 1 lit. d RODO).
Kradzież tożsamości lub oszustwo dotyczące tożsamości	Kradzież tożsamości lub oszustwo dotyczące tożsamości (oraz wiążącego się z tym naruszenia prawa karnego) może nastąpić w razie nieuprawnionego dostępu do danych osobowych (naruszenia zasady zasada integralności i poufności danych, art. 5 ust. 1 lit. f RODO) lub przetwarzania danych osobowych bez podstawy prawnej (przy naruszeniu art. 6, 9 lub 10 RODO, w zależności od kategorii danych). Aby brać pod uwagę możliwość wystąpienia kradzieży tożsamości, ryzyko nieuprawnionego dostępu lub przetwarzania danych bez podstawy prawnej musi dotyczyć takiego zakresu danych, który pozwala na dokonanie tego rodzaju czynu (np. podrobienie dowodu osobistego).
Naruszenie zakazu dyskryminacji	Dotyczy to takiego sposobu przetwarzania danych, który może powodować naruszenie zakazu dyskryminacji osób fizycznych z uwagi na cechę, która zalicza się do danych osobowych. W szczególności chodzi o dyskryminację ze względu na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub skutkujący środkami mającymi taki efekt (motyw 75 RODO). Samo RODO nie zawiera zakazu dyskryminacji, w związku z czym należy zidentyfikować podstawę prawą takiego zakazu.
Szkoda finansowa	Dotyczy to takiego naruszenia ochrony danych osobowych, które może spowodować szkodę finansową osoby, której dane dotyczą.
Szkoda wizerunkowa	Dotyczy to takiego naruszenia ochrony danych osobowych, które może spowodować szkodę wizerunkową osoby, której dane dotyczą. Chodzi tu o taką szkodę wizerunkową, która wynika z naruszenia prawa do prywatności lub innych przepisów służących ochronie reputacji (np. art. 23 Kodeksu cywilnego).
Złamanie tajemnicy zawodowej	Dotyczy to takiego naruszenia ochrony danych osobowych, które skutkuje złamaniem prawnego obowiązku zachowania tajemnicy (np. adwokatów, lekarzy).
Wszelkie inne naruszenia praw i wolności osób fizycznych	Wśród przykładów innych, mniej typowych naruszeń, można wymienić nieuprawnione odwrócenie pseudonimizacji (motyw 85 RODO) oraz naruszenia wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu (motyw 4 RODO).
Wyjaśnienie 5.2. lit. a)-f)	
Jak wskazać źródła ryzyka?	Należy odpowiedzieć, czy i dlaczego istnieją przesłanki do stwierdzenia zagrożenia danym naruszeniem praw i wolności osób, których dane dotyczą (np. ryzyko wycieku danych). W tym celu, należy wykorzystać wnioski z dotychczasowej analizy danego procesu lub operacji przetwarzania oraz zasobów uczestniczących w operacjach przetwarzania.

Jak sporządzić opis potencjalnej szkody?	Należy opisać potencjalne negatywne skutki wystąpienia incydentu, stanowiące naruszenie danej kategorii praw i wolności.
Jak oszacować wagę zagrożenia?	Należy ocenić powagę potencjalnej szkody w skali 1-5. Gdy nie stwierdzono zagrożenia lub ze względu na specyfikę procesu dana kategoria naruszenia nie może wystąpić, należy wybrać odpowiedzieć "brak" lub „nie dotyczy".
Jak oszacować PRAWDOPODOBIEŃSTWO wystąpienia danej szkody?	Należy ocenić prawdopodobieństwo wystąpienia danej szkody w skali 1-5 lub wybrać odpowiedzieć "brak" lub „nie dotyczy".
Jak obliczyć POZIOM RYZYKA?	Należy obliczyć poziom ryzyka w skali 1-9. Poziom ryzyka stanowi iloczyn wagi zagrożenia i prawdopodobieństwa wystąpienia.
Jak wydać rekomendacje?	Należy opisać, w jaki sposób zminimalizować ryzyko naruszenia praw i wolności.

5.3. ADO dokonuje zgłoszenia naruszenia organowi nadzorczemu (Prezes Urzędu Ochrony Danych Osobowych w sposób opisany na stronie PUODO https://uodo.gov.pl/) w terminie 72 godzin od stwierdzenia naruszenia **jeżeli PRAWDOPODOBIEŃSTWO wystąpienia którejkolwiek ze szkód zostało, zgodnie z pkt. 5.2., oszacowane na „4" lub „5" w skali 1-5.** W tym celu, należy skompletować dokumentację naruszenia ochrony danych osobowych, i przesłać ją do organu bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia[1]. W razie przekroczenia terminu 72 godzin, do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia. Jeżeli - i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

5.4. ADO dokonuje zgłoszenia naruszenia osobie, której dane dotyczą bez zbędnej - **jeżeli POZIOM RYZYKA związany z którąkolwiek kategorią naruszenia został, zgodnie z ust. 5.2., oszacowany co najmniej na „6" w skali 1-9. Aby sprawdzić, czy o naruszeniu ochrony danych osobowych należy zawiadomić osoby**, których dotyczą dane dotknięte naruszeniem., w tym celu, odpowiedzieć na pytania zawarte w poniższej tabelce:

Pytanie	Odpowiedź
Czy pomimo wystąpienia naruszenia, dane osobowe objęte są takimi środkami technicznymi i organizacyjnymi, które uniemożliwiają osobom nieuprawnionym dostęp do tych danych?	**[Tak/Nie]**
Czy natychmiast po wykryciu naruszenia zastosowano środki, które powodują, że poziom ryzyka oszacowany zgodnie z pkt. 5.2., w żadnym z przypadków nie przekracza już „5"?	**[Tak/Nie]**

5.5. Jeżeli na żadne z pytań, o których mowa w pkt. 5.4., nie udzielono odpowiedzi twierdzącej, o naruszeniu ochrony danych osobowych należy zawiadomić osoby, których dane dotyczą. Zawiadomienia dokonuje się bez zbędnej zwłoki:

a) osobiście - w formie, która umożliwia wykazanie faktu zawiadomienia, lub
b) w drodze publicznego komunikatu lub podobnego środka, o ile osobiste zawiadomienie każdej z osób, których dane zostały dotknięte naruszeniem, wymagałoby niewspółmiernie dużego wysiłku.

5.6. Zawiadomienie do podmiotu danych wypełnia się jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych i musi:

a) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
c) opisywać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5.7. Zawiadomienie opisane w pkt. 5.4.-5.6. nie jest wymagane gdy:

a) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

[1] Art. 33 ust. 1 RODO.

5.7. Dokonanie zgłoszenia lub zawiadomienia o naruszeniu ochrony danych osobowych odnotowuje się w Rejestrze incydentów i działań korygujących.
5.8. W razie sporządzenia dokumentacji naruszenia ochrony danych osobowych, załącza się ją do Rejestru incydentów i działań korygujących.
5.9. Jeżeli w odniesieniu do operacji przetwarzania dotkniętych naruszeniem ochrony danych osobowych, ADO występuje jako podmiot przetwarzający, naruszenie należy bez zbędnej zwłoki zgłosić administratorowi lub administratorom przedmiotowych danych osobowych. Dokonując zgłoszenia, należy przekazać dokumentację naruszenia ochrony danych osobowych.

6. WDROŻENIE ŚRODKÓW ZARADCZYCH

6.1. Zadania związane z wdrożeniem rekomendacji wydanych stosownie do pkt. 5.2. lit f), należy dodać do Planu utrzymywania i monitorowania zgodności z RODO, wyznaczając do ich realizacji osoby odpowiedzialne.
6.2. W przypadku, gdy zgłoszone naruszenie nie zostało zaklasyfikowane jako naruszenie bezpieczeństwa danych osobowych, ADO powiadamia o tym zgłaszającego.
6.3. W przypadku stwierdzenia działań umyślnych lub wynikłych z nienależytej staranności pracowników i ustaleniu sprawcy naruszenia ochrony danych osobowych bezpośrednio przełożony podejmuje decyzję co do zastosowania środków dyscyplinarnych w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
6.4. ADO, na podstawie rekomendacji IOD lub Zespołu ds. Naruszeń inicjuje działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych.

7. SZKOLENIA

7.1. Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu naruszenia ochrony danych osobowych po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w jednostce o zaistniałym incydencie lub podejrzeniu jego wystąpienia. Dlatego w miarę posiadanych zasobów, co najmniej raz 2 lata należy przeprowadzać okresowe szkolenia pracowników ADO w zakresie zarządzania incydentami naruszenia bezpieczeństwa danych osobowych Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowozatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów naruszenia bezpieczeństwa danych osobowych.

8. ZAŁĄCZNIKI:

ZAŁĄCZNIK NR 1 – Katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych
ZAŁĄCZNIK NR 2 – Nr 2A raport z incydentu naruszającego bezpieczeństwo danych osobowych ze względu na poufność, Nr 2B dostępność i integralność oraz raport z zagrożenia bezpieczeństwa danych
ZAŁĄCZNIK NR 3 – wzór raportu przeglądu

ZAŁĄCZNIK NR 1

Katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

Nr (kod) naruszeń	Formy naruszeń	Sposób postępowania	
		Pracownik Kierownika komórki organizacyjnej	IOD
A **Formy naruszenia danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych**			
A.1	**W zakresie wiedzy**		
A.1.1	Ujawnienie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
A.1.2	Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
A.1.3	Dopuszczenie i stwarzanie warunków, aby ktokolwiek mógł pozyskać informację o sprzęcie i pozostałej infrastrukturze informatycznej np. z obserwacji lub dokumentacji.	Natychmiast przerwać czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
A.2	**W zakresie sprzętu i oprogramowania**		
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Pouczyć osobę, która dopuściła do takiej sytuacji. Przekazać informacje do IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika i sporządza raport.

A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła się do takiej sytuacji. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika

A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska pracy. Ustalić jakie czynności zostały wykonane przez osobę nieuprawnioną Niezwłocznie powiadomić IOD.	Sporządza raport.
A.2.5	Samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa informatyka lub administratora systemu informatycznego w celu odinstalowania programów. Sporządza raport.
A.2.6	Zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa informatyka lub administratora systemu informatyczne w celu przywrócenia stanu pierwotnego. Sporządza raport.
A.2.7	Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy.	Wzywa informatyka lub administratora systemu informatycznego w celu wykonania kontroli antywirusowej. Sporządza raport.
A.2.8	Wykorzystanie ogólnodostępnych serwisów pocztowych (np. Wirtualna Polska, Onet.pl, o2.pl)w celach służbowych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.

A.2.9	Wykorzystanie służbowej poczty elektronicznej do celów prywatnych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.3	**W zakresie dokumentów i obrazów zawierające dane osobowe**		
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od kierownika komórki organizacyjnej /pracownika
A.3.2	Przechowywanie dokumentów w niedostatecznym stopniu zabezpieczonych przed dostępem osób niepowołanych.	Spowodować poprawienie zabezpieczeń. Przekazać informacje do IOD.	Przyjmuje raport od kierownika komórki organizacyjnej / pracownika
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika
A.3.4	Dopuszczenie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika
A.3.5	Dopuszczenie aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawniona osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane – sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacji nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD.	Przyjmuje informacje od kierownika jednostki organizacyjnej/pracownika
A.3.7	Utrata kontroli nad kopią danych osobowych (zgubienie pendrive).	Podjąć próbę odzyskania kopii. Powiadomić IOD.	Przyjmuje informacje raport od kierownika komórki organizacyjnej/pracownika
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**		

A.4.1	Opuszczenie i pozostawienie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Sporządzić raport. Powiadomić IOD.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika

A.4.2	Wpuszczenie do pomieszczenia osób nieznanych i dopuszczenie ich do kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika
A.4.3	Dopuszczenie, aby osoby spoza informatyków/ASI i telekomunikacyjnych podłączały jakiejkolwiek urządzenia do sieci komputerowej, demontowały elementy obudów do gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
A.4.4	Pozostawienie otwartych okien, drzwi po zakończeniu pracy.	Zabezpieczyć (zamknąć) pomieszczenie. Sporządzić raport. IOD.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika
A.4.5	Pożar, zalanie.	Podjąć próbę odzyskania dokumentacji i sprzętu. Powiadomić IOD.	Przyjmuje informacje od kierownika jednostki organizacyjnej/pracownika
A.4.6	Nieprzestrzeganie polityki czystego biurka oraz czystego ekranu	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.4.7	Pozostawienie dokumentów w koszu na śmieci.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od kierownika komórki organizacyjnej/pracownika.
A.4.8	Pozostawienie wydruków na ogólnodostępne drukarce.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od kierownika komórki organizacyjnej/pracownika

A.4.9	Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
A.4.10	Wyniesienie kluczy od pomieszczeń biurowych po zakończonej pracy.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.

A.5	**W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci**		
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiejkolwiek manipulacji przy urządzeniach lub okablowaniach sieci komputerowej w miejscach publicznych (hole, korytarze, itp)	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić informatyka i IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika.
A.5.2	Dopuszczenie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu .	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić informatyka i IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika
B **Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych**			
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika Sporządza raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu lub pochodzeniu.	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.

B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Powiadomić IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika

B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD oraz informatyka.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.
B.7	Zidentyfikowano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośnik.)	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.
B.8	Wykorzystano niezinwentaryzowany środek przetwarzania informacji (nie będący własnością pracodawcy).	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.
B.9	Przechowywanie haseł w niewłaściwy sposób.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD oraz informatyka.	Wzywa informatyka/ASI w celu przywrócenia stanu pierwotnego. Sporządza raport
B.10	Przekazywanie haseł innym osobom.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD oraz informatyka.	Wzywa informatyka/ASI w celu przywrócenia stanu pierwotnego. Sporządza raport.

B.11	Pojawienie się nieautoryzowanej informacji na stronie internetowej.	Powiadomić niezwłocznie informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Powiadomić IOD oraz informatyka.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika
B.12	Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD oraz informatyka.	Wzywa informatyka/ASI w celu przywrócenia stanu pierwotnego. Sporządza raport.
B.13	Wykorzystanie służbowych środków przetwarzania informacj do celów prywatnych.	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji	Sporządza raport.

B.14	Nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy.	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika Sporządza raport.
B.15	Nieuprawniona zmiana danych lub ich uszkodzenie.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD oraz informatyka.	Sporządza raport.
B.16	Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.
B.17	Kradzież sprzętu przetwarzającego informacje.	Niezwłocznie powiadomić IOD oraz informatyka.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika
B.18	Błędy w obsłudze i konserwacji sprzętu komputerowego służącego do przetwarzania informacji.	Powiadomić niezwłocznie IOD oraz informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika. Sporządza raport.

B.19	W wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika Sporządza raport.
B.20	Nieuprawniony dostęp do strefy administracyjnej.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić IOD oraz informatyka. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika.
C **Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**			
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić IOD	Przyjmuje informacje od kierownika komórki organizacyjnej/pracownika
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić IOD .Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika.
C.3	Nie wykonanie kopii zapasowych	Powiadomić IOD oraz informatyka. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika.
C.4	Nie zweryfikowanie możliwości odtworzenia danych z kopii zapasowych.	Powiadomić IOD oraz informatyka. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej/pracownika

ZAŁACZNIK NR 2A

Raport z incydentu naruszającego bezpieczeństwo danych osobowych ze względu na poufność, dostępność i integralność

Sporządzający raport

Imię i nazwisko	
stanowisko (funkcja)	
Dział, pokój nr	

Kod formy naruszenia ochrony danych ..... (wg tabeli) *lub jeżeli nie podpada pod dany incydent własnymi słowami* .....
.....

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):
.....
.....
2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):
.....
.....
3) Osoby , które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:
.....
.....
4) Informacje o danych, które zostały lub mogły zostać ujawnione:
.....
.....
5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
.....
.....
6) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania korekcyjne, korygujące, zapobiegawcze):
.....
.....
.....
.....

DATA:.....GODZINA..... Podpis:

ZAŁACZNIK NR 2B

Raport z zagrożenia bezpieczeństwo danych osobowych

Sporządzający raport

Imię i nazwisko	
stanowisko (funkcja)	
Dział, pokój nr	

Kod formy zagrożenia ochrony danych ..... (wg tabeli) *lub jeżeli nie podpada pod dany incydent własnymi słowami* .....
.....

1) Miejsce, dokładny czas i data stwierdzenia zagrożenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):
.....
.....

2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do zagrożenia ochrony danych osobowych):
.....
.....

3) Osoby , które uczestniczyły w zdarzeniu związanym z zagrożeniem ochrony danych osobowych:
.....
.....

4) Informacje o danych, które mogły zostać ujawnione:
.....
.....

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
.....
.....

6) Krótki opis wydarzenia związanego z zagrożeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania zapobiegawcze):
.....
.....
.....

Data:.....GODZINA.... Podpis:

ZAŁĄCZNIK NR 3

Raport z przeglądu zagrożeń/incydentów bezpieczeństwa danych osobowych

RAPORT Z PRZEGLĄDU ZAGROŻEŃ/INCYDENTÓW	Nr przeglądu
	Data sporządzenia raportu
Data przeprowadzenia przeglądu	
Podsumowanie wyników przeglądu:	
Spostrzeżenia służące doskonaleniu:	

....

PRZEBIEG PRZYKŁADOWEJ KONTROLI

SYSTEMU OCHRONY DANYCH OSOBOWYCH

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Ochrony Danych Osobowych jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
2.	DOKUMENTACJA	Sprawdzenie, czy osoba ma upoważnienie do przetwarzania danych osobowych – upoważnienie powinno odzwierciedlać zakres obowiązków.
3.	DOKUMENTACJA	Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, ale nie przetwarzają tych danych, posiadają zgody na przebywanie w obszarze przetwarzania.
4.	DOKUMENTACJA	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
5.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe czy stosują się do - „zasady czystego biurka" - polityki drukowania, - zamykania dokumentów i pomieszczeń, - ochrony przenośnych urządzeń,
6.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie (jeśli tak - można sporządzić dokumentację fotograficzną pomieszczeń, która stanowić będzie załącznik do poniższego sprawdzenia).
7.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli takie urządzanie nie znajduje się w pomieszczeniu, należy skontrolować pracownika, w jaki sposób niszczy zbędną dokumentację, która nie podlega archiwizacji). Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są przypadkiem wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny lub manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.
8.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.
9.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy systemy komputerowe służące do przetwarzania danych osobowych zapamiętują wszelakie czynności, jakich dokonuje się przy przetwarzaniu danych osobowych.
10.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w programie komputerowym bazodanowym (czyli dotyczącym baz danych) logują się za pomocą WŁASNEGO identyfikatora i hasła.
11.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.
12.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.
13.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.
14.	REJESTR CZYNNOSCI	Kontrolowanie, czy rejestr czynności przetwarzania danych jest aktualny
15.	OBOWIĄZEK INFORMACYJNY	Sprawdzenie, czy ADO wykonuje na bieżąco obowiązki z art. 13-14 RODO

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
16.	PRAWA PODMIOTÓW DANYCH	Przeprowadzenie wywiadu, którego celem jest ustalenie, czy ADO na bieżąco realizuje wnioski i prawa podmiotów danych. Ocena rejestru wniosków.
17.	NARUSZENIE BEZPIECZEŃSTWA	Analiza rejestry naruszeń, Przeprowadzenie wywiadu, którego celem jest ustalenie, czy w ADO na bieżąco zgłaszane są incydenty naruszenia i wykonywane są prawa i obowiązki z art. 33-34 RODO.
18.	ZABEZPIECZENIA ANLIZA RYZYKA z art. 24/32 RODO	Zweryfikowanie czy poprzednia analiza ryzyka jest aktualna, czy trzeba ją ponowić
19.	DPIA	Zweryfikowanie czy procesy przetwarzania danych osobowych wymagające DPIA miały tę ocenę przeprowadzoną, czy projektuje się nowe procesy wymagające tej oceny
20.	ZGODNOŚĆ Z ZASADAMI PRZETWARZANIA DANYCH OSOBOWYCH	Ustalenie czy w każdy proces przetwarzania danych osobowych następuje zgodnie z art. 5 RODO w szczególności co do minimalizacji danych, minimalizacji okresu przetwarzania.
21.	PODMIOTY PRZETWARZAJACE	Zweryfikowanie czy wszędzie tam, gdzie zachodzi powierzenie zawarte są umowy, weryfikacja rejestru umów powierzenia.
22.	UDOSTĘPNIENIE	Zweryfikowanie czy dane osobowe są udostępniane zgodnie z Polityką Ochrony Danych i przepisami prawa.
23.	REJESTR CZYNNOŚCI PRZETWARZANIA	Zweryfikowanie czy Rejestr czynności przetwarzania jest aktualny.
24.	KONTROLA PRAKTYKI	Przeprowadzenie analizy pod kątem pracowników - jakie obecnie mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: • próby nieuprawnionego dostępu do danych osobowych; • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; • próba nieuprawnionej interwencji przy sprzęcie komputerowym; • wynoszenie niezabezpieczonych pamięci z miejsca pracy; • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

L.P.	**ZAGADNIENIA /** **OBOWIĄZUJĄCE WYMAGANIA /** **ZAKRES KONTROLI**	**REKOMENDACJE / ZALECENIA**	**STAN FAKTYCZNY / UWAGI / Odpowiedzi: TAK, NIE lub NIE DOTYCZY/ Dodatkowe uszczegółowienie odpowiedzi /** **ZALECANE ROZWIĄZANIA**
SRODKI OCHRONY W RAMACH NARZĘDZI PROGRAMOWYCH – ustalenie czy programy służące do przetwarzania danych spełniają wymagania RODO (część obowiązków może być realizowana przez człowieka np. prawo do przenoszenia danych itp., to zależy od funkcjonalności systemu i decyzji ADO)			

	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach bazy danych.	Rozliczalności – rozumiana jako właściwość zapewniająca, że działania użytkownika mogą być przypisane w sposób jednoznaczny tylko temu użytkownikowi; Integralności danych – rozumiana jako właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany; Mechanizm audytowania zdarzeń.	
	Rozliczalność w systemie podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).	W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.	
	Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych	Polityka kontroli dostępu. Przydzielanie dostępu użytkownikom oraz przegląd praw dostępu użytkowników. Odbieranie lub dostosowywanie praw dostępu. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbioru danych osobowych dla poszczególnych użytkowników systemu informatycznego.	
	W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych – uwierzytelnianie.	Dostęp do zbioru danych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Identyfikacja osób dokonujących wpisu.	
	Obowiązujące u Dostawcy zasady zarządzania uprawnieniami powinny w szczególności uwzględniać zagrożenia związane z nieprawidłowym wykorzystaniem uprawnień użytkowników uprzywilejowanych. Dostawca powinien przeanalizować stopień narażenia na ryzyko w zakresie bezpieczeństwa		

	swojego środowiska i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia mechanizmów zapewniających każdorazową rejestrację oraz możliwość monitorowania dostępu z poziomu uprawnień uprzywilejowanych do najbardziej wrażliwych komponentów środowiska teleinformatycznego.		
	Systemy informatyczne przetwarzające dane o wysokiej istotności dla towarzystwa powinny posiadać mechanizmy pozwalające na automatyczną rejestrację zachodzących w nich zdarzeń w taki sposób, aby zapisy tych rejestrów mogły – w przypadku wystąpienia takiej konieczności – stanowić wiarygodne dowody niewłaściwego lub niezgodnego z zakresem zadań użytkowników korzystania z tych systemów. Mechanizmy rejestracji zdarzeń powinny również uniemożliwiać nieuprawnione usuwanie lub modyfikowanie zapisów.		
	Reguły zarządzania ruchem sieciowym powinny zostać sformalizowane, podobnie jak reguły rejestrowania zdarzeń przez narzędzia monitorujące bezpieczeństwo infrastruktury teleinformatycznej i informowania o tych zdarzeniach. Zdarzenia te powinny podlegać systematycznej analizie. Dostawca powinien posiadać dokumentację analizy złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska, na podstawie której pojęto decyzję o zastosowaniu (lub niezastosowaniu) rozwiązań klasy IDS / IPS (ang. Intrusion Detection System / Intrusion Prevention System), zwiększających bezpieczeństwo infrastruktury teleinformatycznej poprzez wykrywanie (IDS) lub wykrywanie i blokowanie (IPS) ataków w czasie rzeczywistym.	System IDS/IPS do ochrony dostępu do sieci komputerowej. Serwer proxy pozwalający na analizę ruchu sieciowego oraz dostępu do sieci Internet. Blokowany dostęp do niepowołanych stron.	
	Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten zapewnia odnotowanie:	1) daty pierwszego wprowadzenia danych do systemu; 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu; 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą; 4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;	

		5) sprzeciwu co do dalszego przetwarzania danych.	
	Zastosowano kryptograficzne środki ochrony danych osobowych	Szyfrowane połączenia (np. VPN). Pseudonimizacja i szyfrowanie danych osobowych.	
	Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego	Procedura tworzenia, przechowywania, testowania zapasowych kopii bezpieczeństwa (Czy system wykonuje kopie zapasowe?). Procedura odtworzenia systemu na wypadek awarii. Plan ciągłości działania.	
	Asysta techniczna - zakres asysty i warunki. Czy w ramach serwisowania platformy dostawca ma dostęp do danych osobowych przetwarzanych w systemie? – Obowiązki procesora – podmiotu przetwarzającego.	Umowa serwisowa, warunki gwarancji. Umowa powierzenia przetwarzania danych. Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.	
	zabezpieczenie danych przed uszkodzeniem lub utratą	monitorowanie dostępu do informacji, zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Mechanizm audytowania zdarzeń.	
	zachowanie integralności i wiarygodności danych	Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Zachowanie spójności danych i wykrywanie zmian.	
Funkcjonalność uwzględniająca nowe obowiązki administratora oraz uprawnienia podmiotów danych			
	Prawo do sprostowania/uzupełnienia danych		
	Prawo do usunięcia danych (prawo do bycia zapomnianym). Prawo do sprzeciwu	Należy ustalić kto będzie podejmować decyzje o usunięciu danych i czy system jest w stanie zlokalizować i usunąć żądane dane. Osoba, której dane dotyczą, ma prawo w określonych przypadkach żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez	

		zbędnej zwłoki usunąć dane osobowe. Jeżeli administrator upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje	
	Prawo do przenoszenia danych	Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.	
	Prawo do tego, by nie podlegać profilowaniu	Osoba, której dane dotyczą, ma prawo, by nie podlegać decyzji opierających się na przetwarzaniu zautomatyzowanym – w tym profilowaniu, i wywołującej dla niej określone skutki prawne (np. brak możliwości udzielenia kredytu czy zawarcia umowy ubezpieczenia).	

Regulamin Ochrony Danych Osobowych w Państwowej Wyższej Szkole Zawodowej im. Witelona w Legnicy

§ 1.
Postanowienia ogólne

1. Celem wprowadzenia Regulaminu jest ustalenie podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla pracowników i innych osób wykonujących prace na rzecz Uczelni, mających dostęp do danych osobowych przetwarzanych przez Administratora
2. Definicje zawarte w dokumencie „Polityka ochrony danych osobowych w Państwowej Wyższej Szkole Zawodowej im Witelona w Legnicy" stosuje się odpowiednio.

§ 2.
Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie, otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. studentom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych.
5. Dostęp osób nieupoważnionych do drukarek na których drukowane są dane osobowe powinien być odpowiednio ograniczony.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   1) wylogować się z systemu informatycznego oraz wyłączyć sprzęt komputerowy.
   2) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. Wychodząc z pomieszczenia, w którym przetwarzane są dane należy sprawdzić czy zamknięte są okna i wejście do pomieszczenia.
8. Osoby użytkujące laptopa, tablet bądź służbowy smartfon, służący do przetwarzania danych osobowych, obowiązane są zabezpieczyć hasłem dostęp do tych urządzeń oraz zachować szczególną ostrożność podczas ich transportu i przechowywania.

§ 3.
Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Każdy Użytkownik przystępujący do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, wpisuje swój indywidualny przydzielony przez ASI login oraz właściwe hasło dostępu.
2. Główny informatyk lub osoba przez niego upoważniona tj. ASI przekazując użytkownikowi login i hasło przeprowadza szkolenie z zakresu pracy oraz bezpieczeństwa danych w systemie informatycznym.
3. Użytkownicy nie mogą korzystać z innych loginów niż te, do których są upoważnieni.
4. Użytkownik ma obowiązek wylogowania się lub zablokowania systemu w przypadku nieobecności na stanowisku pracy lub w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim użytkownika.

§ 4.
Polityka haseł

1. Hasło ustanowione podczas przyznawania uprawnień przez ASI należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
2. Hasło powinno składać się z co najmniej ośmiu znaków, zawierać małe i duże litery oraz cyfry lub znaki specjalne.
3. Hasło użytkownika ulega automatycznej zmianie raz na 30 dni. Za jego zmianę odpowiedzialny jest użytkownik.
4. Hasło nie powinno być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła, należy go natychmiast zmienić. W razie problemów powiadomić o tym fakcie ASI.
6. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego loginu i hasła.

§ 5.
Zabezpieczenie dokumentów z danymi osobowymi

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione.
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
4. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów, np. w szafach, biurkach, pomieszczeniach, przed kradzieżą lub wglądem osób nieupoważnionych.
5. Wydruki, notatki, kserokopie dokumentów itp. nie wykorzystane a zawierające dane osobowe muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
6. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
7. Pracownik który odpowiada za przechowywanie wydruku zawierającego dane osobowe, może przekazać wydruk oraz odpowiedzialność za jego przechowanie innej osobie tylko wtedy, gdy jest ona upoważniona do dostępu informacji zawartych na wydruku.
8. Pracownik nie może wynosić na zewnątrz elektronicznych nośników informacji, a także papierowych dokumentów z zapisanymi danymi osobowymi bez zgody Rektora lub Kanclerza.
9. Po uzyskaniu zgody Rektora lub Kanclerza, dane osobowe wynoszone na nośnikach elektronicznych poza miejsce pracy muszą być zaszyfrowane.

§ 6.
Zasady korzystania z Internetu oraz poczty elektronicznej

1. Pracownik zobowiązany jest do korzystania z Internetu oraz poczty elektronicznej wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach.
3. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo).
4. Przesyłanie danych osobowych z użyciem maila poza Uczelnię może odbywać się tylko przez osoby do tego upoważnione.
5. W przypadku przesyłania danych osobowych poza Uczelnię należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
6. Zabrania się otwierać załączniki oraz klikać w hiperlinki otrzymane od nieznanych nadawców wiadomości e-mail. Otrzymanie podejrzanych wiadomości należy niezwłocznie zgłosić ASI.
7. Podczas wysyłania wiadomości elektronicznej do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".
8. Użytkownik bez zgody Rektora lub Kanclerza nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące ADO, jego pracowników, studentów lub kontrahentów za pośrednictwem Internetu, w tym również przy użyciu prywatnej elektronicznej skrzynki pocztowej.

§ 7.
Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do niezwłocznego powiadomienia Inspektora Ochrony Danych Osobowych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
   4) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   5) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
   6) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

§ 8.
Obowiązek zachowania poufności i ochrony danych osobowych

1. Każdy Pracownik dopuszczony do przetwarzania danych osobowych jest zobowiązany do:
   1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę zadaniach;
   2) zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę;
   3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę;
   4) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Udostępnienie danych osobowych instytucjom, osobom spoza Uczelni może odbywać się wyłącznie na pisemny uzasadniony wniosek, za zgodą Rektora lub Kanclerza.
3. Zabrania się udostępniania danych osobowych bezpośrednio oraz telefonicznie bez weryfikacji tożsamości osoby proszącej o dane osobowe oraz podstawy do udzielenia informacji.

§ 9.
Zasady korzystania ze służbowej poczty elektronicznej

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych administratora danych podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna niezwiązana z działalnością Administratora powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.
6. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).
7. Zabronione jest:
   1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
   2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
   3) odbieranie przesyłek z nieznanych źródeł;
   4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;
   6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
   7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
   8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego,
   9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy,
   10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

§ 10.
Zasady korzystania z sieci publicznej

1. Sieć, w której pracują urządzenia komputerowe Administratora musi być odseparowana od sieci publicznej zaporą ogniową oraz systemem wykrywania włamań (IPS).
2. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.

3. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
4. Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych, w szczególności połączeń sftp i https.
5. Dostęp użytkowników do sieci publiczne (Internet) jest ograniczony do niezbędnego minimum na danym stanowisku pracy.
6. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.
7. Dostęp do protokołu wymiany plików możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.
8. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez ASI.

§ 11.
Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.