

POLITYKA BEZPIECZEŃSTWA **w zakresie ochrony danych osobowych** **w Uniwersytecie Przyrodniczym we Wrocławiu**

§ 1

Władze Uczelni świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Uczelni swoje dane osobowe do właściwej i skutecznej ochrony tych danych, deklarują zamiar:

- podejmowania wszelkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem przetwarzania danych osobowych,
- stałego podnoszenia kwalifikacji osób przetwarzających dane osobowe w Uczelni w zakresie problematyki bezpieczeństwa przetwarzania tych danych,
- traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonywania przez zatrudnione osoby,
- podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

§ 2

W celu **zapobiegania zagrożeniom** wynikającym z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach teleinformatycznych, związanym z:

- infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą wykradać zasoby tego komputera (zarówno stacjonarne jak i sieciowe),
- dostępem do stron internetowych, na części których zainstalowane są skrypty pozwalające wykradać zasoby komputera,
- ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera,
- użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza Uczelnię,
- spamem, posiadającym niekiedy programy pozwalające wykradać zasoby komputera,
- możliwością niekontrolowanego kopiowania danych na dyski wymienne (np.: CD, pendrive, DVD),
- możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane (oprogramowanie typu sniffer, które może być również instalowane przez wirusy),
- lekceważeniem zasad ochrony danych polegających na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia (np.: bez wylogowania się lub bez zabezpieczenia wygaszacza ekranu hasłem),
- brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy (osób nieuprawnionych do przetwarzania danych),
- atakami z sieci uniemożliwiającymi przetwarzanie (ataki typu DoS na serwery),
- działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
- kradzieżą sprzętu lub nośników z danymi, które zazwyczaj są nie zabezpieczone,
- przekazywaniem sprzętu z danymi do serwisu,
- kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
- podszywaniem się przez osoby nieuprawnione pod witrynę internetową, która zbiera dane i innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem technik i metod

przetwarzania danych, Uczelnia będzie stale doskonaliła i rozwijała organizacyjne, techniczne oraz informatyczne środki ochrony przetwarzanych danych osobowych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom.

§ 3

1. Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dokłada szczególnej staranności w celu **ochrony interesów osób, których dane dotyczą**, a w szczególności zapewnia, aby dane te były:
 - 1) przetwarzane zgodnie z prawem,
 - 2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
 - 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
 - 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Pod szczególną ochroną Uczelni pozostają **wrażliwe dane osobowe** wymienione w art. 27 ust. 1 ustawy.

Przetwarzanie danych: ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjną lub związkowa, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sadowym lub administracyjnym - dopuszczalne jest tylko w związku z realizacją celów statutowych Uczelni i w granicach wynikających z przepisów art. 27 ust. 2 ustawy.

§ 4

1. Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje **odpowiednie środki informatyczne, techniczne i organizacyjne** zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności: zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, Uczelnia dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych.
3. W szczególności Uczelnia zapewnia aktualizację informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz inni zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci teleinformatycznych.

§ 5

1. Uczelnia sprawuje kontrolę i nadzór nad niszczeniem zbędnych danych osobowych i ich zbiorów.
2. **Niszczenie zbędnych danych osobowych** i ich zbiorów polega w szczególności na:
 - 1) trwałym, fizycznym zniszczeniu danych osobowych i ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przy stosowaniu powszechnie dostępnych metod,
 - 2) anonimizacji danych osobowych i ich zbiorów polegającej na pozbawieniu danych osobowych i ich zbiorów cech pozwalających na identyfikację osób fizycznych, których anonimizowane dane dotyczą.
3. Osoby przetwarzające dane osobowe w Uczelni mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych lub ich zbiorów.

4. Naruszanie przez zatrudnione, w ramach stosunku pracy, osoby upoważnione do dostępu i przetwarzania danych osobowych, stosowanych w Uczelni procedur niszczenia zbędnych danych osobowych lub ich zbiorów, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającym stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.
5. Kontrola i nadzór nad niszczeniem zbędnych danych osobowych lub ich zbiorów może w szczególności polegać na wprowadzeniu odpowiednich procedur niszczenia danych, a także zleceniu niszczenia ich, wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.

§ 6

Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych prowadzi dokumentację opisującą **sposób przetwarzania danych oraz środki ochrony tych danych**. W skład tej dokumentacji wchodzi w szczególności:

- zarządzenia rektora w sprawie bezpieczeństwa danych osobowych zawierające jako integralne części:
 - a) Politykę bezpieczeństwa w zakresie ochrony danych osobowych,
 - b) Instrukcję zarządzania systemami informatycznymi używanymi do przetwarzania danych osobowych,
 - c) Instrukcję postępowania w przypadkach naruszenia ochrony danych osobowych,
- inne pisma, instrukcje szczegółowe i polecenia służbowe określające procedury mające znaczenie dla ochrony danych osobowych – wydawane przez ADO i upoważnione podmioty.

§ 7

1. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, **Uczelnia udostępnia przetwarzane na jej obszarze dane osobowe wyłącznie osobom do tego upoważnionym** na mocy uregulowań wewnętrznych.
2. Upoważnienie, o którym mowa w ust. 1, wynikać może w szczególności:
 - a) z charakteru pracy wykonywanej na danym stanowisku pracy,
 - b) z zakresu obowiązków wykonywanych na danym stanowisku pracy,
 - c) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

§ 8

Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia **dostęp do przetwarzanych danych osobowych** osobom fizycznym będącym dysponentami tych danych.

§ 9

1. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika Uczelni.
2. Zasada wyrażona w ust. 1. ma także zastosowanie do przypadku korzystania przez związki zawodowe z uprawnień przysługujących im na mocy ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity z 1998 r.: Dz.U. Nr 21, poz. 94 ze zmianami) i ustawy z dnia 23 maja 1991 r. o związkach zawodowych (tekst jednolity z 2001 r. Dz. U. Nr 79, poz. 854 ze zmianami).

§ 10

1. Zarządy związków zawodowych działających w Uczelni mogą, do celów analitycznych i studyjnych, uzyskiwać w administracji Uczelni informacje o zarobkach pracowników w formie anonimowej, uniemożliwiającej określenie tożsamości pracowników.

2. Dział Kadr i Spraw Socjalnych udostępnia dane osobowe pracownika zarządowi związku zawodowego, jeśli związek ten zostanie wskazany przez pracownika jako jego rzecznik. Na udostępnienie informacji o wysokości wynagrodzenia pracownik wyraża odrębnie zgodę na piśmie.
3. Kierownik każdej jednostki organizacyjnej Uczelni informuje podległych sobie pracowników o przysługujących im prawach do kontroli przetwarzania ich danych osobowych, w trybie rozdziału 4 ustawy.

§ 11

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia ADO lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. W szczególności dostęp do danych osobowych na wskazanej w ust. 1 zasadzie mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień – wszystkie – po okazaniu dokumentów potwierdzających te uprawnienia.

§ 12

1. Dane osobowe udostępnia się na piśmie, umotywowany wniosek, chyba że przepis ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
2. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§ 13

1. **Dane osobowe aktualnych pracowników Uczelni** są przetwarzane w Dziale Kadr i Spraw Socjalnych, który udostępnia dane przełożonym pracownika oraz właściwym organom Uczelni, a także – po zatwierdzeniu rektora lub innej upoważnionej przez niego osoby – innym uprawnionym instytucjom (w szczególności sądom, policji, prokuraturze i organom kontrolującym). Dane osobowe pracowników korzystających z Biblioteki – przetwarza Biblioteka Główna.
2. **Dane osobowe byłych pracowników Uczelni** są przetwarzane w okresie do jednego roku po ustaniu stosunku pracy – w Dziale Kadr i Spraw Socjalnych, a po upływie tego okresu – w Archiwum Uczelni zgodnie z odrębnymi przepisami o działalności archiwalnej (ustawa z dnia 14 lipca 1983 r., Dz. U. Nr 38, poz. 173 ze zmianami). Dane osobowe żyjących byłych pracowników są udostępniane organom Uczelni, a także uprawnionym instytucjom w trybie przewidzianym w § 12 ust. 1. Dane osobowe byłych pracowników są udostępniane także historykom i biografom za zgodą rektora lub innej, upoważnionej przez niego osoby.
3. **Dane osobowe byłych pracowników Uczelni będących emerytami lub rencistami** przetwarzane są w Dziale Kadr i Spraw Socjalnych w celach realizacji uprawnień do korzystania z funduszu socjalnego – na ich imienny wniosek – corocznie, do końca życia.
4. Dział Kadr i Spraw Socjalnych przetwarza również **dane osobowe dzieci** pozostających na utrzymaniu (do 25. roku życia – jeżeli się uczą) pracowników, oraz byłych pracowników Uczelni będących emerytami lub rencistami, zgodnie z uprawnieniami wynikającymi z regulaminu zakładowego funduszu świadczeń socjalnych.
5. Dane osobowe dotyczące finansów są przetwarzane w kwesturze.
6. Dane osobowe dotyczące planowania i rozliczania zajęć dydaktycznych przetwarzane są w jednostkach, w których realizowane są te zajęcia oraz w Dziale Organizacji Studiów.

7. Jednostki organizacyjne Uczelni przetwarzają dane osobowe swych pracowników w zakresie niezbędnym do zapewnienia prawidłowej działalności jednostki.

§ 14

1. **Dane osobowe pracownika są udostępniane publicznie** (np. na tablicy ogłoszeń, w składzie osobowym lub w Internecie) jedynie w zakresie:
 - a) stopni naukowych i stanowiska, miejsca zatrudnienia i funkcji pełnionych w Uczelni,
 - b) zajęć dydaktycznych (w stosunku do nauczycieli akademickich),
 - c) sprawy kandydowania w wyborach do organów Uczelni, niezbędnych do tego informacji (w szczególności życiorysu w brzmieniu ustalonym przez kandydata) i wyników wyborów,
 - d) odznaczeń, nagród i wyróżnień (bez wskazania kwot pieniężnych).
2. Wysokość wynagrodzenia pracownika dostępna jest, poza upoważnionym personelem służb finansowych i kadrowych Uczelni, przełożonym pracownika, a w przypadku wynagrodzenia z tytułu umowy o dzieło lub umowy zlecenia – dodatkowo kierującemu daną pracą.
3. Informacje o bieżących przychodach pracownika (tzw. "paski" listy płac) i roczne rozliczenia przychodów (PIT-y) są wydawane do rąk własnych zainteresowanemu pracownikowi lub osobie przez niego upoważnionej – bezpośrednio przez upoważniony personel Działu Płac i Świadczeń Społecznych, albo za pośrednictwem przełożonego pracownika.
4. Dane osobowe osób ubiegających się o świadczenia socjalne, w tym wysokość wynagrodzeń oraz sytuacja materialna i życiowa rodziny, są udostępniane członkom komisji socjalnej opiniującej przyznawanie świadczeń socjalnych.
5. Dostęp do danych osobowych zawartych w dokumentacji dotyczącej regulacji płac ma rektor, kanclerz i personel przygotowujący technicznie listy regulacji płac, chyba że rektor upoważni również przełożonych pracownika.

§ 15

1. **Dane osobowe studentów** Uczelni są przetwarzane w:
 - Dziale Organizacji Studiów,
 - Dziale Spraw Studenckich,
 - Dziale Nauki,
 - dziekanatach poszczególnych wydziałów,
 - Centrum Kształcenia na Odległość,
 - Centrum Sieci Komputerowych,
 - Kwesturze,
 - Bibliotece Głównej.
2. W jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną przetwarza się dane osobowe studentów w zakresie niezbędnym do zapewnienia prawidłowego toku studiów.
3. Informacji o danych osobowych studentów udziela się w dziekanacie lub w dziale, o którym mowa w ust. 1, tylko w odpowiedzi na pisemny wniosek organów Uczelni, a po zatwierdzeniu dziekana lub kierownika działu, także innym uprawnionym instytucjom (w szczególności sądom, policji, prokuraturze i organom kontrolnym).
4. Wszyscy pracownicy mający dostęp do indeksów i protokołów egzaminacyjnych (w szczególności nauczyciele akademicy oraz personel dziekanatów i działów) są zobowiązani do odpowiedniego zabezpieczenia tych dokumentów przed osobami trzecimi.
5. Dziekan wydziału lub inna osoba upoważniona przez ADO Uczelni informuje studentów o przysługujących im, zgodnie z rozdziałem 4 ustawy, prawach do kontroli przetwarzania ich danych osobowych.
6. Postanowienia ust. 1-5 stosuje się odpowiednio do słuchaczy studiów podyplomowych i kursów specjalistycznych organizowanych przez Uczelnię.

§ 16

1. **Dane osobowe kandydatów na studia** przetwarzane są w:

- komisjach rekrutacyjnych,
 - Dziale Organizacji Studiów,
 - dziekanatach poszczególnych wydziałów,
 - Centrum Sieci Komputerowych,
 - Kwesturze.
2. W kwestionariuszu-podaniu, składanym przez kandydata ubiegającego się o przyjęcie na studia umieszcza się informację o celu zbierania danych osobowych i o ich późniejszym przetwarzaniu, łącznie z umieszczeniem łącznie z umieszczeniem numeru PESEL na liście zawierającej wyniki rekrutacji. Kandydat podpisuje odpowiednie oświadczenie zawierające jego zgodę na przetwarzanie w Uczelni jego danych osobowych w zakresie niezbędnym do realizacji toku studiów oraz w celu wydania elektronicznej legitymacji studenckiej w Centrum Personalizacji Środowiskowej Elektronicznej Legitymacji Studenckiej Uczelni Wrocławia. Informację o uprawnieniach kandydatów, zgodnie z rozdziałem 4 ustawy, umieszcza się w widocznym miejscu na tablicach informacyjnych dotyczących rekrutacji.
 3. Wyniki rekrutacji ogłasza się na listach zawierających numery PESEL kandydatów. Informacji telefonicznych i za pomocą poczty elektronicznej o wynikach rekrutacji udziela się po podaniu nazwiska i numeru PESEL kandydata.
 4. Dane osobowe kandydatów na studia, którzy nie zostali przyjęci, usuwa się po zakończeniu procesu rekrutacji, a pozostałe przekazuje się do bazy danych systemu dziekanatowego.

§ 17

1. **Dane osobowe absolwentów**, są przetwarzane w jednostkach, o których mowa w § 15 ust. 1, w okresie dwóch lat od daty ukończenia studiów, a po upływie tego okresu dane te przetwarza się w Archiwum, zgodnie z przepisami o działalności archiwalnej (ustawa z dnia 14 lipca 1983 r., Dz. U. Nr 38, poz. 173 ze zmianami).
2. Dane osobowe słuchaczy studiów podyplomowych, kursów lub szkoleń przetwarzane w jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną, a po upływie dwóch lat od daty ukończenia studiów, kursu lub szkolenia są przekazywane do Archiwum w zakresie ustalonym przepisami ustawy, o której mowa w ust. 1.
3. W jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną są przechowywane wykazy wyników nauczania studentów. W tych danych studenci są identyfikowani jedynie imieniem, nazwiskiem i numerem albumu.
4. Postanowienia ust. 1-3 stosuje się odpowiednio do osób, które przerwały studia, kursy lub szkolenia przed uzyskaniem dyplomu lub zaświadczenia o ukończeniu studiów (kursów, szkoleń).

§ 18

Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia kontrolę nad dostępem do tych danych. Kontrola ta w szczególności realizowana jest poprzez **ewidencjonowanie osób przetwarzających dane osobowe** oraz wdrożenie procedur udzielania dostępu do tych danych.

§ 19

1. Uczelnia zapewnia **zaznajomienie osób upoważnionych do dostępu i przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa**, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Uczelni.
2. W szczególności osoby, wskazane w ust. 1, zaznajamiane są z zagadnieniami wymienionymi w tym przepisie przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych osobowych, a także odpowiednio, w trakcie trwania zatrudnienia w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub technikach i środkach ochrony danych stosowanych w Uczelni.
3. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i

środkami ochrony tych danych stosowanymi w Uczelni może odbywać się w szczególności poprzez:

- 1) instruktaż na stanowisku pracy,
- 2) szkolenie wewnętrzne realizowane na terenie Uczelni,
- 3) szkolenie zewnętrzne.

§ 20

Osoby upoważnione do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o **powinności zachowania w tajemnicy danych osobowych** oraz sposobów ich zabezpieczenia stosowanych w Uczelni.

§ 21

1. Uczelnia gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów statutowych, realizację uprawnień gwarantowanych im przez obowiązujące przepisy prawa.
2. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacją celów statutowych Uczelni, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych na zasadach określonych w art. 32-35 ustawy.
3. Osoby fizyczne, których dane osobowe są przetwarzane w związku z realizacją celów statutowych Uczelni, uzyskują informację o przysługujących im prawach w sposób przyjęty w Uczelni.

§ 22

1. Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza **budynki, pomieszczenia i części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe.**
2. W przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.
3. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności dokonane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych uniemożliwiający lub co najmniej ograniczający niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
4. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego Uczelni, w szczególności stacje robocze (poszczególne komputery) wchodzące w skład tego systemu. Powinny one być usytuowane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa Szczegółowa Polityka Bezpieczeństwa Uczelni, dostępna u ADO.
6. W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar Uczelni, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych.
7. Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w budynkach,

pomieszczeniach i częściach pomieszczeń, tworzących obszar Uczelni, w którym przetwarzane są dane osobowe – wyłącznie w obecności upoważnionego pracownika Uczelni, lub w razie jego nieobecności – na podstawie upoważnienia wydanego przez ADO lub lokalnego administratora.

§ 23

1. Całkowite **opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe przez osobę przetwarzającą te dane**, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
2. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe przez osobę przetwarzającą te dane, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających przetwarzane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzania danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym, uniemożliwiających dostęp do danych osobowych osobom niepowołanym.
3. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

§ 24

1. **Dostęp do budynków i pomieszczeń Uczelni, w których przetwarzane są dane osobowe podlega kontroli.**
2. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdanienia klucza.
3. Klucze do pomieszczeń, w których przetwarzane są dane osobowe mogą być wydawane wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do pomieszczeń na innych zasadach.
4. Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
5. Szczegółowe zasady kontroli dostępu do poszczególnych obszarów (budynków i pomieszczeń) Uczelni, w których przetwarzane są dane osobowe określone są przez osoby kierujące poszczególnymi jednostkami organizacyjnymi Uczelni, w których takie obszary występują.

§ 25

1. Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje **nadzór nad rodzajami oraz zawartością zbiorów danych osobowych** tworzonych na jego obszarze.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem:
 - struktury zbiorów danych,
 - zawartości poszczególnych pól informacyjnych i powiązań między nimi,
 - programów zastosowanych do przetwarzania tych danych,określa Szczegółowa Polityka Bezpieczeństwa Uczelni.

§ 26

1. Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zgodną z przepisami rozdziału 5 ustawy **ochronę zbiorów danych osobowych sporządzanych**

doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką realizowaną w Uczelni, a po ich wykorzystaniu niezwłoczne usunięcie albo poddanie anonimizacji.

2. Osoby, które posiadają zbiory danych osobowych sporządzone doraźnie, dla nieistniejącego już celu (brak aktualnego upoważnienia), są zobowiązane do niezwłocznego usunięcia tych danych.

§ 27

Uczelnia realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych **zabrania tworzenia zbiorów danych osobowych**, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych **innych niż niezbędne dla realizacji celów statutowych Uczelni**.