Załącznik nr 1 do Zarządzenia Rektora UKSW nr 16/2010
z dnia 8 kwietnia 2010 r.

POLITYKA BEZPIECZEŃSTWA
w zakresie ochrony danych osobowych
na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie

§ 1

Władze Uniwersytetu świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Uniwersytetowi swoje dane osobowe do właściwej i skutecznej ochrony tych danych, deklarują podejmowanie niezbędnych działań dla zapewnienia:
- bezpieczeństwa przetwarzania danych osobowych,
- stałego podnoszenia kwalifikacji osób przetwarzających dane osobowe 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,
- współpracy z instytucjami powołanymi do ochrony danych osobowych.

§ 2

1. 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 Uniwersytetem,
   - spamem, posiadającym niekiedy programy pozwalające wykradać zasoby komputera,
   - możliwością niekontrolowanego kopiowania danych na dyski wymienne (np.: CD, 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 związanego z dopuszczeniem 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 nie są 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.
   - Uniwersytet będzie stale doskonalił i rozwijał organizacyjne, techniczne oraz informatyczne środki ochrony przetwarzanych danych osobowych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom.

§ 3

1. Uniwersytet, 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 Uniwersytetu pozostają wrażliwe dane osobowe wymienione w art. 27 ust. 1 ustawy.
3. Przetwarzanie danych: ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, 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 sądowym lub administracyjnym – jest dopuszczalne tylko w związku z realizacją celów statutowych Uniwersytetu i w granicach wynikających z przepisów art. 27 ust. 2 ustawy.

§ 4

1. Uniwersytet 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, Uniwersytet dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych.
3. W szczególności Uniwersytet zapewnia aktualizację informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz innymi zagrożeniami danych, płynącymi z funkcjonowania systemów informatycznych oraz sieci teleinformatycznych.

§ 5

1. Uniwersytet 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 Uniwersytecie 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 Uniwersytecie 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 zlecaniu ich niszczenia wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.
6. Dane zarchiwizowane w archiwum Uniwersytetu niszczone są zgodnie z procedurami określonymi w instrukcji archiwizacji.

§ 6

Uniwersytet, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki ochrony tych danych. W skład tej dokumentacji wchodzą w szczególności:

1) zarządzenia rektora w sprawie ochrony danych osobowych i baz danych w systemach informatycznych, 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;
2) 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, Uniwersytet udostępnia przetwarzane na jego obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań wewnętrznych.
2. Upoważnienie, o którym mowa w ust. 1, wynikać może w szczególności:
   1) z charakteru pracy wykonywanej na danym stanowisku pracy,
   2) z zakresu obowiązków wykonywanych na danym stanowisku pracy,
   3) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

§ 8

Uniwersytet, 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 na pisemny wniosek, wyłącznie w obecności upoważnionego pracownika Uniwersytetu, na zasadach określonych w art. 29 i 30 ustawy.
2. Zasada wyrażona w ust. 1 ma także zastosowanie w 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 na Uniwersytecie mogą, do celów analitycznych i studyjnych, uzyskiwać w administracji Uniwersytetu 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 Uniwersytetu 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 przedstawiciele: Państwowej Inspekcji Pracy, Zakładu Ubezpieczeń Społecznych, organów skarbowych, Policji, Agencji Bezpieczeństwa Wewnętrznego, sądów powszechnych, Najwyższej Izby Kontroli,

Generalnego Inspektora Ochrony Danych Osobowych i innych upoważnionych przez przepisy prawa podmiotów i organów, działający w granicach przyznanych im uprawnień – wszyscy – po okazaniu dokumentów potwierdzających te uprawnienia.

§ 12

1. Dane osobowe udostępnia się na pisemny, 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 Uniwersytetu są przetwarzane w Dziale Kadr i Spraw Socjalnych, który udostępnia dane przełożonym pracownika oraz właściwym organom Uniwersytetu, 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 Uniwersytetu, oraz biblioteki specjalistyczne.
2. Dane osobowe byłych pracowników Uniwersytetu są przetwarzane w okresie do jednego roku po ustaniu stosunku pracy – w Dziale Kadr i Spraw Socjalnych, a po upływie tego okresu – w Archiwum Uniwersytetu zgodnie z odrębnymi przepisami o działalności archiwalnej (ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach Dz. U. 2006 r. Nr 97, poz. 673 z późniejszymi zmianami). Dane osobowe żyjących byłych pracowników są udostępniane organom Uniwersytetu, 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 Uniwersytetu 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.
4. Dział Kadr i Spraw Socjalnych przetwarza również dane osobowe dzieci pozostających na utrzymaniu pracowników (dzieci do 21. roku życia – jeżeli się uczą).
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 Kształcenia.
7. Dane osobowe dotyczące autorów publikacji wydawanych w Wydawnictwie UKSW, przetwarzane są w Wydawnictwie UKSW.
8. Jednostki organizacyjne Uniwersytetu 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:
   1) stopni naukowych i stanowiska, miejsca zatrudnienia i funkcji pełnionych w Uniwersytecie,
   2) zajęć dydaktycznych (w stosunku do nauczycieli akademickich),
   3) sprawy kandydowania w wyborach do organów Uniwersytetu, niezbędnych do tego informacji (w szczególności życiorysu w brzmieniu ustalonym przez kandydata) i wyników wyborów,
   4) odznaczeń, nagród i wyróżnień (bez wskazania kwot pieniężnych).
2. Wysokość wynagrodzenia pracownika dostępna jest, poza upoważnionym personelem służb finansowych i kadrowych Uniwersytetu, 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.
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 i doktorantów Uniwersytetu są przetwarzane w:
   - Dziale Kształcenia,
   - Biurze Rekrutacji,
   - Biurze ds. Badań Naukowych,
   - dziekanatach poszczególnych wydziałów,
   - Dziale Pomocy Materialnej dla Studentów,
   - Centrum Systemów Informatycznych,
   - Kwesturze,
   - Bibliotece Uniwersytetu.
2. W jednostkach organizacyjnych Uniwersytetu 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 organom Uniwersytetu, 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 akademiccy oraz personel dziekanatów i działów) są zobowiązani do odpowiedniego zabezpieczenia tych dokumentów przed osobami trzecimi.
5. Dziekan wydziału lub inna osoba upoważniona przez ADO 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 wszystkich stopni i rodzajów studiów, studiów podyplomowych oraz kursów dokształcających organizowanych przez Uniwersytet.

§ 16

1. Dane osobowe kandydatów na studia przetwarzane są w:
   - komisjach rekrutacyjnych,
   - Biurze Rekrutacji,
   - dziekanatach poszczególnych wydziałów,
   - Centrum Systemów Informatycznych,
   - Kwesturze.
2. W kwestionariuszu składanym przez kandydata na studia umieszcza się informację o celu zbierania danych osobowych i o ich późniejszym przetwarzaniu oraz informację o umieszczeniu numeru PESEL kandydata na liście zawierającej wyniki rekrutacji. Kandydat podpisuje odpowiednie oświadczenie zawierające jego zgodę na przetwarzanie jego danych osobowych w zakresie niezbędnym do realizacji toku studiów na Uniwersytecie oraz w celu wydania elektronicznej legitymacji studenckiej. 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 o wynikach rekrutacji udziela się przez telefon i za pomocą poczty elektronicznej wyłącznie 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 w dziekanatach .

§ 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 archiwizuje się i przetwarza w Archiwum, zgodnie z przepisami o działalności archiwalnej (ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach Dz. U. 2006 r. Nr 97, poz. 673 z późniejszymi zmianami).

2. Dane osobowe słuchaczy studiów podyplomowych, kursów lub szkoleń przetwarzane w jednostkach organizacyjnych Uniwersytetu 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 Uniwersytetu 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

Uniwersytet, 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. Uniwersytet 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.
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.
3. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych może odbywać się w szczególności poprzez:
   1) instruktaż na stanowisku pracy,
   2) szkolenie wewnętrzne realizowane na terenie Uniwersytetu,
   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 sposobach ich zabezpieczenia.

§ 21

1. Uniwersytet 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 Uniwersytetu, 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 Uniwersytetu, uzyskują informację o przysługujących im prawach.

§ 22

1. Uniwersytet, 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 cześć 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 uniemożliwiające lub co najmniej ograniczające 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 Uniwersytetu, 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 Uniwersytetu, dostępna u ADO.
6. W budynkach, pomieszczeniach i częściach pomieszczeń tworzących obszar Uniwersytetu, 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 Uniwersytetu, w którym przetwarzane są dane osobowe – wyłącznie w obecności upoważnionego pracownika Uniwersytetu, 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 przetwarzana 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 Uniwersytetu, 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 zdania 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. Uniwersytet 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) Uniwersytetu, w których przetwarzane są dane osobowe, określane są przez osoby kierujące poszczególnymi jednostkami organizacyjnymi Uniwersytetu, w których takie obszary występują.

§ 25

1. Uniwersytet, 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 Uniwersytetu.

§ 26

1. Uniwersytet, 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 na Uniwersytecie, 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

Uniwersytet, 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 jego celów statutowych.