Załącznik Nr 2
do Zarządzenia Nr 54/2009
z dnia 06.07.2009 r.
Rektora SUM

Zarządzenie Nr 66/2006
z dnia 14.06.2006 r.
Rektora
Śląskiego Uniwersytetu Medycznego w Katowicach

w sprawie: ochrony danych osobowych przetwarzanych w Śląskim Uniwersytecie Medycznym w Katowicach.

tekst jednolity

Działając na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. Nr 164, poz. 1365 z późn. zm.), art. 2 i 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jedn*. Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz 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. z 2004 r. Nr 100, poz. 1024) zarządzam, co następuje:

I. Administrator Danych Osobowych

§ 1

Śląski Uniwersytet Medyczny w Katowicach jest administratorem danych osobowych w rozumieniu przepisów ustawy o ochronie danych osobowych *(t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)*, a czynności w sprawach z zakresu ochrony danych osobowych dokonuje **Rektor,** jeżeli co innego nie wynika z postanowień niniejszego zarządzenia.

II. Lokalni Administratorzy Danych Osobowych

§ 2

1. Tworzy się strukturę Lokalnych Administratorów Danych Osobowych, którym przekazuje się – odpowiednio do zakresu realizowanych przez nich celów statutowych – obowiązki i uprawnienia administratora danych osobowych w rozumieniu § 1 niniejszego zarządzenia.
2. Lokalnymi Administratorami Danych Osobowych są:
   a) Dziekan Wydziału Lekarskiego w Katowicach,
   b) Dziekan Wydziału Opieki Zdrowotnej w Katowicach,
   c) Dziekan Wydziału Lekarskiego z Oddziałem Lekarsko – Dentystycznym w Zabrzu,
   d) Dziekan Wydziału Farmaceutycznego z Oddziałem Medycyny Laboratoryjnej w Sosnowcu,
   e) Dziekan Wydziału Zdrowia Publicznego w Bytomiu,
   f) Dyrektor Biblioteki Śląskiego Uniwersytetu Medycznego w Katowicach,
   g) Kanclerz Śląskiego Uniwersytetu Medycznego w Katowicach.

3. W związku z postanowieniem ust. 1 i 2, za przetwarzanie danych osobowych oraz ich ochronę odpowiedzialni są:
   a) Dziekani Wydziałów w zakresie danych osobowych przetwarzanych w ramach Wydziałów SUM,
   b) Dyrektor Biblioteki Śląskiego Uniwersytetu Medycznego w Katowicach w zakresie danych osobowych przetwarzanych w Bibliotece SUM,
   c) Kanclerz Śląskiego Uniwersytetu Medycznego w Katowicach w zakresie danych osobowych przetwarzanych w podporządkowanych organizacyjnie jednostkach i samodzielnych stanowiskach pracy administracji i obsługi Uczelni, zgodnie z §121 ust. 1 Statutu Śląskiego Uniwersytetu Medycznego w Katowicach.
4. Lokalny Administrator Danych Osobowych jest zobowiązany dołożyć szczególnej staranności w celu ochrony przetwarzanych danych osobowych, a w szczególności, aby były one:
   a) Przetwarzane zgodnie z prawem,
   b) Zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, niezgodnemu z tymi celami,
   c) Merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane,
   d) Przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
5. Lokalny Administrator Danych Osobowych zobowiązany jest do:
   a) Stworzenia właściwych warunków organizacyjno – technicznych zapewniających ochronę danych osobowych w podległej jednostce organizacyjnej, a szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą uszkodzeniem lub zniszczeniem.
   b) Zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

III. Pełnomocnik Rektora ds. Ochrony Danych Osobowych

§ 3

1. Powołuje się Pełnomocnika Rektora ds. Ochrony Danych Osobowych w Śląskim Uniwersytecie Medycznym w Katowicach, zwanego dalej „Pełnomocnikiem ds. Ochrony Danych Osobowych."
   Pełnomocnikiem ds. Ochrony Danych Osobowych będzie Zastępca Pełnomocnika Rektora ds. Ochrony Informacji Niejawnych.
2. Pełnomocnik ds. Ochrony Danych Osobowych podlega bezpośrednio Rektorowi.
3. Zadaniem Pełnomocnika ds. Ochrony Danych Osobowych jest nadzorowanie i koordynowanie w Uczelni zasad postępowania przy przetwarzaniu danych osobowych, a w szczególności:
   a) Opracowanie i bieżącą aktualizację Polityki Bezpieczeństwa,
   b) Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w Uczelni, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą uszkodzeniem lub zniszczeniem,

c) Zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane,
d) Klasyfikowanie zbiorów danych osobowych przetwarzanych w Uczelni,
e) Przedstawianie Rektorowi SUM do podpisania dokumentu „Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych",
f) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
g) Wnioskowanie o usunięcie uchybień w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych,
h) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
i) Prowadzenie ewidencji miejsc przetwarzania danych osobowych i sposobu ich zabezpieczenia,
j) Prowadzenie ewidencji udostępnionych danych osobowych na wniosek osób lub podmiotów skierowany w sprawie pracowników jednostek organizacyjnych podporządkowanych Kanclerzowi SUM,
k) Opracowanie programu szkoleń w zakresie ochrony danych osobowych.

4. Pełnomocnik ds. Ochrony Danych Osobowych współpracuje w zakresie postępowania przy przetwarzaniu danych osobowych z następującymi osobami funkcyjnymi:
   a) Pełnomocnikami Lokalnych Administratorów Danych Osobowych,
   b) Administratorem Bezpieczeństwa Informacji.

IV. Pełnomocnicy Lokalnych Administratorów Danych Osobowych

§ 4

1. Wyznacza się Pełnomocników Lokalnych Administratorów Danych Osobowych, o których mowa w § 2 ust. 2.
2. Pełnomocnikami Lokalnych Administratorów Danych Osobowych są:
   a) W Wydziałach SUM – kierownicy dziekanatów,
   b) W Bibliotece SUM – Zastępca Dyrektora Biblioteki,
   c) W stosunku do jednostek organizacyjnych administracji podległych bezpośrednio Rektorowi SUM a także Kanclerzowi SUM, zadania te wykonuje Pełnomocnik ds. Ochrony Danych Osobowych.
3. Do zadań Pełnomocników Lokalnych Administratorów Danych Osobowych należy:
   a) Prowadzenie ewidencji danych osobowych udostępnionych przez Lokalnego Administratora Danych Osobowych na wniosek osób lub podmiotów,
   b) Zgłaszanie Pełnomocnikowi ds. Ochrony Danych Osobowych osób, które upoważniono do przetwarzania danych osobowych w celu ujęcia w ewidencji,
   c) Przedstawianie propozycji nowego zbioru danych osobowych podlegającego rejestracji u Generalnego Inspektora Ochrony Danych Osobowych,
   d) Zapoznawanie osób upoważnionych do przetwarzania danych osobowych ze zmianami w obowiązujących przepisach,
   e) W przypadku naruszenia bezpieczeństwa danych osobowych zgłoszenie tego faktu Lokalnemu Administratorowi Danych Osobowych i Pełnomocnikowi ds. Ochrony Danych Osobowych, przeprowadzenie analizy okoliczności i przyczyn, które doprowadziły do naruszenia obowiązujących przepisów i wnioskowanie o wprowadzenie niezbędnych zabezpieczeń.

V. Administrator Bezpieczeństwa Informacji

§ 5

1. W Śląskim Uniwersytecie Medycznym w Katowicach wyznacza się Administratora Bezpieczeństwa Informacji (ABI). ABI odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Uczelni, nadzoruje przestrzeganie zasad ochrony tych danych, przeciwdziała dostępowi do systemów informatycznych Uczelni osób nieupoważnionych do przetwarzania danych osobowych w SUM. W przypadku wykrycia naruszeń w systemie zabezpieczeń, odpowiada za podjęcie właściwych działań. Funkcję Administratora Bezpieczeństwa Informacji pełnić będzie Zastępca Kierownika Centrum Informatyki i Informatyzacji.
2. Do podstawowych zadań ABI należy:
   a) Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
   b) Dopilnowanie, aby wprowadzane środki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych były zgodne z przepisami 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 systemu informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024),
   c) Nadzorowanie procedur wykonywania przeglądów, serwisowania, konserwowania oraz likwidacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych osobowych,
   d) Zarządzanie środkami uwierzytelniania użytkowników i nadzorowanie przestrzegania procedur użytkowania opisanych w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Śląskim Uniwersytecie Medycznym w Katowicach" wprowadzonej Zarządzeniem Rektora SUM Nr 84/2007 z dnia 14.09.2007 roku,
   e) Nadzorowanie sposobu zabezpieczenia systemów informatycznych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do danych, utratą danych osobowych w wyniku awarii zasilania lub zakłóceniami w sieci zasilającej, wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
   f) Nadzorowanie wykonywania kopii zapasowych, ich przechowywania oraz okresowego sprawdzania pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemów,
   g) Nadzorowanie systemu komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji,
   h) Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu lub informacji o zmianach w sposobie działania programu lub urządzeń, które wskazują na naruszenie bezpieczeństwa danych,
   i) Analizowanie sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych osobowych i przygotowanie w porozumieniu z Pełnomocnikiem ds. Ochrony Danych Osobowych propozycji zmian do „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Śląskim Uniwersytecie Medycznym w Katowicach"

zwiększających bezpieczeństwo przetwarzanych danych oraz przedstawienie ich Rektorowi SUM,

j) Inicjowanie przedsięwzięć zmierzających do doskonalenia bezpieczeństwa przetwarzanych danych osobowych i w porozumieniu z Pełnomocnikiem ds. Ochrony Danych Osobowych podejmowanie właściwych działań.

3. Administratorowi Bezpieczeństwa Informacji podlegają Administratorzy Systemów Informatycznych (ASI) wyznaczeni z grona pracowników Centrum Informacji i Informatyzacji, którzy realizują bezpośrednio obowiązki Administratora Bezpieczeństwa Informacji w wyznaczonym przez ABI obszarze działania. Szczegółowy zakres obowiązków ASI określa Polityka Bezpieczeństwa.

VI. Przetwarzanie danych osobowych.

§ 6

1. Przetwarzanie danych osobowych w Śląskim Uniwersytecie Medycznym w Katowicach odbywa się w związku z realizacją zadań wynikających z art. 13 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym *(Dz. U. Nr 164, poz. 1365 z późn. zm.)*.
2. Przetwarzanie danych osobowych w SUM jest realizowane w systemach informatycznych oraz kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych przez pracowników upoważnionych do przetwarzania danych osobowych.
3. W zakresie przetwarzania danych osobowych stosuje się odpowiednio przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.*) oraz wewnętrzne akty prawne wprowadzone zarządzeniami Rektora SUM.
4. Każdej osobie przysługuje prawo do kontroli przetwarzanych danych, które jej dotyczą, zawartych w zbiorach danych Śląskiego Uniwersytetu Medycznego w Katowicach.
5. Pracownicy SUM upoważnieni do przetwarzania danych osobowych dopełnią szczególnej staranności w pracy nie dopuszczając do ich udostępnienia osobom nieupoważnionym, zabrania przez osobę nieuprawnioną, nieuzasadnionej modyfikacji oraz zmiany, uszkodzenia lub zniszczenia.
6. Pracownicy SUM przetwarzający dane osobowe zobowiązani są do zachowania ich w tajemnicy również po ustaniu zatrudnienia.
7. Zobowiązuje się kierowników wszystkich jednostek organizacyjnej Uczelni do:
   a) Szkolenia podległych pracowników (w tym nowo zatrudnionych) przetwarzających dane osobowe z zakresu obowiązujących przepisów o ochronie danych osobowych oraz odpowiedzialności pracownika za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem,
   b) Nadzorowania przestrzegania zaleceń „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Śląskim Uniwersytecie Medycznym w Katowicach" – załącznika do Zarządzenia Nr 84/2007 z dnia 14.09.2007 r. Rektora SUM,
   c) Dopilnowania, aby pracownicy przetwarzający dane osobowe posiadali stosowne upoważnienia.

VII. Upoważnienie do przetwarzania danych osobowych.

§ 7

1. Przetwarzanie danych osobowych w Śląskim Uniwersytecie Medycznym w Katowicach mogą realizować wyłącznie pracownicy upoważnieni do przetwarzania danych osobowych. Upoważnienie wydaje Lokalny Administrator Danych Osobowych, o którym mowa w § 2 ust. 2 niniejszego zarządzenia (wzór upoważnienia przedstawia załącznik Nr 1 do zarządzenia) na wniosek kierownika jednostki organizacyjnej, bezpośredniego przełożonego zatrudnianego pracownika.
2. Ewidencję osób upoważnionych w SUM do przetwarzania danych osobowych prowadzi Pełnomocnik ds. Ochrony Danych Osobowych.
3. Upoważnienia, o których mowa w ust. 1, wykonuje się w dwóch egzemplarzach. Po podpisaniu przez pracownika, kierownika jednostki organizacyjnej (bezpośredniego przełożonego danego pracownika) i Lokalnego Administratora Danych Osobowych przesyła się je Pełnomocnikowi ds. Ochrony Danych Osobowych. Pełnomocnik, po ujęciu ich w „Ewidencji osób upoważnionych do przetwarzania danych osobowych w SUM" przekazuje jeden egzemplarz upoważnienia do Działu ds. Pracowniczych i Socjalnych, drugi egzemplarz otrzymuje upoważniona osoba.

VIII. Udostępnienie danych osobowych

§ 8

1. Upoważnia się Lokalnych Administratorów Danych Osobowych do udostępniania danych osobowych zgromadzonych w zbiorach SUM osobom i podmiotom, w sposób określony w art. 29 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.) w obszarach wymienionych w § 2 ust. 3.
2. Dane osobowe udostępnia się na pisemny umotywowany wniosek, zawierający informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych, wskazujący ich zakres i przeznaczenie oraz podstawę prawną wniosku.
3. Ewidencję udostępnionych danych osobowych prowadzą: Pełnomocnik ds. Ochrony Danych Osobowych oraz Pełnomocnicy Lokalnych Administratorów Danych Osobowych w obszarach wymienionych w § 2 ust. 3.
4. Kopię wniosku o udostępnienie danych osobowych wraz z odpowiedzą, przekazuje się odpowiednio Pełnomocnikowi ds. Ochrony Danych Osobowych lub Pełnomocnikowi Lokalnego Administratora Danych Osobowych.

IX. Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 9

1. Przez naruszenie ochrony danych osobowych rozumie się:
   a) Stwierdzone naruszenie zabezpieczenia systemu informatycznego,
   b) Sytuacje, gdy stan urządzeń, zawartość zbioru danych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczenia danych,

c) Stwierdzone naruszenie zabezpieczenia dokumentacji w formie papierowej, zaginięcie dokumentu, próba jego powielenia lub wyniesienia bez zgody przełożonego,
d) Udostępnienie osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzanie z naruszeniem ustawy oraz zmianę, utratę, uszkodzenie lub zniszczenie.

2. Każdy pracownik SUM, a w szczególności osoba upoważniona do przetwarzania danych osobowych jest obowiązana niezwłocznie powiadomić o zaistniałym przypadku naruszenia ochrony danych osobowych bezpośredniego przełożonego, a ten odpowiednio Pełnomocnika ds. Ochrony Danych Osobowych lub Pełnomocnika Lokalnego Administratora Danych Osobowych.
3. O przypadku naruszenia ochrony danych osobowych Pełnomocnik ds. Ochrony Danych Osobowych lub Pełnomocnik Lokalnego Administratora Danych Osobowych jest obowiązany zawiadomić odpowiednio Rektora SUM lub Lokalnego Administratora Danych Osobowych wymienionego w § 2 ust. 2, a także:
   a) Zarejestrować fakt naruszenia danych osobowych, podając miejsce, datę i przypuszczalny zakres ich naruszenia,
   b) Podjąć natychmiastowe działania zmierzające do usunięcia stwierdzonych niedociągnięć,
   c) Ustalić osobę odpowiedzialną za zaistniałą sytuację,
   d) Przeprowadzić analizę aktualnego sposobu zabezpieczenia danych,
   e) Przedstawić propozycję naprawy systemu, która uniemożliwi w przyszłości naruszenie ochrony danych.
4. W razie stwierdzenia, że dane osobowe zostały udostępnione osobom lub podmiotom w sposób niezgodny z obowiązującymi przepisami lub zabrane przez osobę nieuprawnioną Pełnomocnik Lokalnego Administratora Danych osobowych niezwłocznie zawiadamia o tym Pełnomocnika ds. Ochrony Danych Osobowych.
5. Pełnomocnik ds. Ochrony Danych Osobowych w porozumieniu z Administratorem Bezpieczeństwa Informacji przygotowuje Rektorowi SUM pisemny wniosek do osoby lub podmiotu o zwrot lub usunięcie danych osobowych, w których posiadanie weszły niezgodnie z prawem.

X. Ochrona danych osobowych zgromadzonych w toku rekrutacji na studia w Śląskim Uniwersytecie Medycznym w Katowicach

§ 10

1. Członkowie Uczelnianej Komisji Rekrutacyjnej (UKR), Wydziałowych Komisji Rekrutacyjnych (WKR), Komisji Egzaminacyjnych oraz wyznaczeni pracownicy SUM mogą przetwarzać dane osobowe zgromadzone w czasie rekrutacji, pod warunkiem posiadania aktualnego upoważnienia do przetwarzania danych osobowych wydanego na okres rekrutacji.
2. Upoważnienie, o którym mowa w § 10 ust. 1 wydaje Lokalny Administrator Danych Osobowych przed rozpoczęciem rekrutacji.
3. Zobowiązuje się członków Uczelnianej Komisji Rekrutacyjnej, Wydziałowych Komisji Rekrutacyjnych, Komisji Egzaminacyjnych oraz wyznaczonych pracowników SUM do przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz innych aktualnych aktów prawnych.

4. W komputerach znajdujących się w pomieszczeniach przeznaczonych dla UKR i WKR wykorzystywanych w procesie rekrutacji, podłączonych do sieci internetowej, należy zastosować na poziomie wysokim środki bezpieczeństwa określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjny, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
5. Dane osobowe przetwarzane w procesie rekrutacji do komputera wprowadzają wyłącznie członkowie wyżej wymienionych komisji oraz wyznaczeni pracownicy SUM posiadający stosowne upoważnienie do przetwarzania danych osobowych.
6. Każdy z członków komisji oraz wyznaczony pracownik powinien dysponować własnym kontem komputerowym zabezpieczonym hasłem znanym tylko i wyłącznie właścicielowi konta. Konto zakłada pracownik Centrum Informatyki i Informatyzacji nadzorujący daną lokalizację właściwą dla UKR i WKR.
7. Komputery używane w procesie rekrutacji przygotowuje Centrum Informatyki i Informatyzacji. Zabrania się używania w procesie rekrutacji innych komputerów niż dostarczone i przygotowane do tego celu.
8. Kopie zapasowe danych osobowych należy wykonywać na optycznych, magnetycznych, elektronicznych nośnikach zgodnie z zaleceniami „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Śląskim Uniwersytecie Medycznym w Katowicach" (załącznik Nr 1 do Zarządzenia Nr 84/2007 z dnia 14.09.2007 r. Rektora SUM). Nośnik powinien być przechowywany w pomieszczeniu UKR, WKR w zamkniętej szafie lub kasetce zabezpieczonej przed dostępem osób nieuprawnionych.
9. Pomieszczenia pracy komisji rekrutacyjnych, w każdym przypadku ich opuszczenia powinny być zamykane (również w godzinach pracy).
10. Osoby nieuprawnione mogą przebywać w pomieszczeniach UKR, WKR tylko w obecności osób upoważnionych do przetwarzania danych osobowych w procesie rekrutacji.
11. Sprzątanie pomieszczeń może odbywać się tylko w obecności osób upoważnionych.
12. Klucze do pomieszczeń UKR, WKR przechowuje się na portierni. Do pobierania i zdawania kluczy do tych pomieszczeń upoważniają wyznaczonych pracowników przewodniczący komisji rekrutacyjnych. Wykaz osób upoważnionych do pobierania kluczy przechowuje się na portierni. Pobieranie i zdawanie kluczy na przechowanie potwierdza się podpisem wraz z datą i godziną w książce ewidencji kluczy.
13. Po zakończeniu postępowania rekrutacyjnego zgromadzoną dokumentację przechowuje się zgodnie z obowiązującymi przepisami.

XI. Postanowienia końcowe

§ 11

Nieprzestrzeganie postanowień niniejszego zarządzenia skutkuje odpowiedzialnością karną, o której mowa w przepisach rozdziału 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz odpowiedzialnością dyscyplinarną określoną w Statucie Śląskiego Uniwersytetu Medycznego w Katowicach oraz Regulaminie Pracy Śląskiego Uniwersytetu Medycznego w Katowicach – załącznik do Zarządzenia Nr 26/2008 z dnia 17.03.2008 roku.

§ 12

Treść niniejszego Zarządzenia polecam zamieścić na stronie internetowej Uczelni.

§ 13

Tracą moc Zarządzenia: Nr 4/2005 z dnia 1 luty 2005 oraz Nr 18/2005 z dnia 16 marca 2005 r. Rektora Śląskiej Akademii Medycznej w Katowicach.

§ 14

Zarządzenie wchodzi w życie z dniem podpisania.

R E K T O R
Śląskiego Uniwersytetu Medycznego w Katowicach

prof. dr hab. n. med. Ewa Małecka – Tendera

Otrzymują:

- Prorektorzy,
- Lokalni Administratorzy Danych Osobowych (Kanclerz SUM, Dziekani Wydziałów, Dyrektor Biblioteki SUM),
- Pełnomocnicy Lokalnych Administratorów Danych Osobowych (Kierownicy Dziekanatów, Zastępca Dyrektora Biblioteki SUM),
- Pełnomocnik Rektora ds. Ochrony Danych Osobowych,
- Administrator Bezpieczeństwa Informacji,
- a/a.

Do wiadomości:

- Wszystkie jednostki organizacyjne.

Załącznik Nr 1
do Zarządzenia Nr 66/2006
z dnia 14.06.2006 r.
Rektora SUM

Nr ewidencyjny.....
(nadany przez Pełnomocnika ds. Ochrony Danych Osobowych)

UPOWAŻNIENIE
do przetwarzania danych osobowych

I. Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.)*

Upoważniam Panią/Pana .....
(imię i nazwisko)

zatrudnioną na stanowisku .....
(nazwa stanowiska i jednostki/komórki organizacyjnej)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na wyżej wymienionym stanowisku w systemie tradycyjnym (kartoteki, ewidencje, rejestry, spisy itp.) i informatycznym w zakresie: wgląd/pełny zakres*, w terminie……..……..….. .
(od-do/ na czas nieokreślony)

.....
(podpis Lokalnego Administratora Danych Osobowych)

OŚWIADCZENIE PRACOWNIKA

II.

Ja niżej podpisany (na) oświadczam, iż:

1) Zostałam(em) przeszkolona(ny) w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926) i 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. z 2004 r. Nr 100, poz. 1024), oraz innych obowiązujących w SUM aktów prawnych.
2) Zobowiązuję się:
   a) Zachować w tajemnicy dane osobowe, z którymi zetknęłam się/zetknąłem się w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy jak i po jego ustaniu;
   b) Chronić dane osobowe przed dostępem osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, ujawnieniem, uszkodzeniem lub zniszczeniem.

.....
(podpis pracownika)

.....
(podpis bezpośredniego przełożonego)

- niepotrzebne skreślić