



ZARZĄDZENIE

Nr 6/2012

**Rektora
Uniwersytetu Marii Curie-Skłodowskiej
w Lublinie**

z dnia 7 lutego 2012 r.

***w sprawie ochrony danych osobowych przetwarzanych
w Uniwersytecie Marii Curie-Skłodowskiej w Lublinie***

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. 3 ustawy z dnia 29 sierpnia 1997 r. - o ochronie danych osobowych (tj. Dz. U. 2002 r., Nr 101, poz. 926 z późn. zm.), 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) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536),

zarządzam:

§ 1

1. Przetwarzanie danych osobowych w Uniwersytecie Marii Curie-Skłodowskiej (zwanym dalej Uniwersytetem) służy realizacji zadań wynikających z art. 13 ust. 1 ustawy z dnia 27 lipca 2005 r.- *Prawo o szkolnictwie wyższym*.
2. Przez przetwarzanie danych osobowych rozumie się jakiegokolwiek operacje wykonywane na danych osobowych pracowników, doktorantów, studentów i absolwentów, kandydatów do pracy oraz kandydatów na studia a w szczególności zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie tych danych.
3. Dane osobowe przetwarza się wyłącznie dla określonych celów związanych z działalnością Uniwersytetu.
4. Dane osobowe mogą być przetwarzane w systemie informatycznym, a także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 2

Ilećroć w niniejszym zarządzeniu jest mowa o:

- 1) danych osobowych – oznacza to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 2) zbiorze danych – oznacza to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 3) administratorze danych – oznacza to podmiot decydujący o celach i środkach przetwarzania danych osobowych;
- 4) administratorze bezpieczeństwa informacji – oznacza to osobę nadzorującą z upoważnienia administratora danych osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.

§ 3

Zadania Administratora Danych Osobowych w Uniwersytecie w rozumieniu ustawy z dnia 29 sierpnia 1997 r. - *o ochronie danych osobowych* realizuje Rektor UMCS.

§ 4

1. Rektor wykonuje obowiązki wynikające z ustawy *o ochronie danych osobowych* w stosunku do podległych mu bezpośrednio stanowisk.
2. Obowiązki wynikające z wyżej wymienionej ustawy w stosunku do pozostałych stanowisk powierza się Lokalnym Administratorom Danych Osobowych.
3. Lokalni Administratorzy Danych Osobowych są bezpośrednio podlegli Administratorowi Danych Osobowych.
4. Lokalnymi Administratorami Danych Osobowych są:
 - 1) prorektorzy;
 - 2) dziekani;
 - 3) kanclerz;
 - 4) kierownicy jednostek ogólnouczelnianych.

§ 5

1. Lokalni Administratorzy Danych Osobowych zobligowani są do podjęcia wszelkich środków organizacyjnych, jak i technicznych, mających na celu pełną ochronę przetwarzanych danych osobowych w podległych im jednostkach organizacyjnych Uniwersytetu.
2. Obowiązki Lokalnych Administratorów Danych Osobowych nie wykraczają poza zakres dotyczący kierowanych przez nich jednostek organizacyjnych Uniwersytetu.
3. Lokalni Administratorzy Danych Osobowych odpowiadają za:
 - 1) wdrożenie, realizację i nadzorowanie „*Polityki bezpieczeństwa danych osobowych w UMCS*” oraz „*Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w UMCS*”;
 - 2) wyznaczenie lokalnych administratorów bezpieczeństwa informacji oraz określenie zakresu ich obowiązków w ramach ochrony danych osobowych w poszczególnych jednostkach organizacyjnych Uniwersytetu;
 - 3) w szczególności:
 - a) dodanie do zakresu czynności osób zatrudnionych przy przetwarzaniu danych osobowych obowiązków, które wynikają z ustawy *o ochronie danych osobowych*,

- b) dopuszczanie do przetwarzania danych osobowych osób do tego upoważnionych,
 - c) kontrolę przestrzegania zasad dotyczących przetwarzania danych osobowych,
 - d) rozpoczynanie i podejmowanie przedsięwzięć mających na celu udoskonalenie ochrony danych osobowych w Uniwersytecie,
 - e) rejestrowanie danych osobowych w podległych im jednostkach organizacyjnych,
 - f) prowadzenie ewidencji miejsc przetwarzania danych osobowych oraz sposobów ich zabezpieczania,
 - g) udostępnianie danych osobowych podmiotom spoza Uniwersytetu oraz prowadzenie ewidencji udostępniania tychże danych osobowych,
 - h) dokonanie klasyfikacji zbiorów danych osobowych przetwarzanych w danej jednostce organizacyjnej.
5. Na wniosek Lokalnego Administratora Danych Osobowych Rektor może powoływać pełnomocników Lokalnego Administratora Danych Osobowych.

§ 6

1. Rektor powołuje Administratora Bezpieczeństwa Informacji w celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w systemach informatycznych Uniwersytetu.
2. Administrator Bezpieczeństwa Informacji podlega bezpośrednio Rektorowi.
3. Na wniosek Administratora Bezpieczeństwa Informacji Rektor powołuje Zastępcę Administratora Bezpieczeństwa Informacji.
4. Zastępca Administratora Bezpieczeństwa Informacji wykonuje zadania i obowiązki w zakresie powierzonym mu przez Administratora Bezpieczeństwa Informacji.

§ 7

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad lokalnymi administratorami bezpieczeństwa informacji w zakresie przetwarzania i ochrony danych osobowych w systemach informatycznych podległych jednostek organizacyjnych.
2. Do zadań Administratora Bezpieczeństwa Informacji należy:
 - 1) opracowanie ***Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie*** oraz ***Polityki bezpieczeństwa danych osobowych w UMCS***;
 - 2) prowadzenie ewidencji wszystkich osób pełniących obowiązki administratorów danych osobowych i administratorów bezpieczeństwa informacji;
 - 3) sprawowanie funkcji kontrolnych w zakresie ochrony danych osobowych w Uniwersytecie;
 - 4) przeciwdziałanie dostępowi osób niepowołanych do systemów, w których przetwarzane są dane osobowe;
 - 5) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
 - 6) przeszkalanie osób przyjmowanych do pracy na stanowiska związane z obsługą systemów informatycznych, służących do przetwarzania danych osobowych;
 - 7) organizowanie i prowadzenie cyklicznych szkoleń dla pracowników zatrudnionych przy przetwarzaniu danych osobowych;
 - 8) określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego;

- 9) zabezpieczenie urządzeń i systemów informatycznych służących do przetwarzania danych osobowych, zasilanych energią elektryczną, przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
- 10) okresowe tworzenie kopii awaryjnych danych osobowych zawartych w systemach informatycznych oraz ich przechowywanie;
- 11) wyposażenie systemów informatycznych przetwarzających dane osobowe w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych;
- 12) ustalenie każdemu użytkownikowi systemu informatycznego odrębnego identyfikatora i hasła umożliwiającego bezpośredni dostęp do przetwarzania danych osobowych;
- 13) monitorowanie wszelkich wydawanych zaleceń GODO, których przedmiotem jest ochrona danych osobowych;
- 14) wprowadzenie wszelkich zaleceń GODO do wewnętrznego systemu ochrony danych osobowych w Uniwersytecie.

§ 8

Zobowiązuje się kierowników jednostek organizacyjnych przetwarzających dane osobowe do:

- 1) opracowania indywidualnych zakresów czynności, określających zakres odpowiedzialności podległych pracowników za ochronę danych osobowych;
- 2) zaznajamiania przyjmowanych do pracy osób z przepisami o ochronie danych osobowych;
- 3) zapewnienia zamykania budynków lub pomieszczeń, w których przetwarzane są dane osobowe, na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.

§ 9

1. Każdemu, którego dane osobowe są przetwarzane, przysługuje prawo do ochrony danych jego dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania lub poprawiania, jak również do uzyskiwania wszelkich informacji o przysługujących mu prawach.
2. Osoby, które zostały upoważnione do przetwarzania danych osobowych są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia.
3. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu.

§ 10

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające specjalne upoważnienie (*załącznik nr 1*), wydane przez Rektora.
2. Szczegółowe zasady uzyskania upoważnienia lub jego cofnięcia zostaną określone przez Administratora Bezpieczeństwa Informacji UMCS w *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w UMCS*.
3. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi na podstawie wydanych upoważnień Dział Organizacyjno-Prawny.
4. Osoba upoważniona do przetwarzania danych osobowych podpisuje oświadczenie o przyjęciu pełnomocnictwa z zakresu ochrony danych osobowych (*załącznik nr 2*), które dołącza się do jej akt osobowych.

5. W przypadku przetwarzania danych osobowych w ramach realizacji projektów współfinansowanych ze środków Unii Europejskiej lub innych środków bezzwrotnych upoważnienia do przetwarzania danych osobowych wydawane są zgodnie z ich wytycznymi.

§ 11

1. Udostępnianie danych osobowych podmiotom spoza Uniwersytetu odbywa się wyłącznie za pośrednictwem Administratora Danych Osobowych lub Lokalnych Administratorów Danych Osobowych.
2. Dane osobowe są udostępniane na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
3. Osoby, o których mowa w ust. 1 udostępniające dane osobowe prowadzą ewidencję udostępniania danych osobowych.

§ 12

Zobowiązuje się pracowników Uniwersytetu, w szczególności upoważnionych do przetwarzania danych osobowych do zapoznania się z niniejszym zarządzeniem.

§ 13

Nadzór nad realizacją niniejszego zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 14

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

prof. dr hab. Andrzej Dąbrowski