ZARZĄDZENIE NR 257/2008
PREZYDENTA MIASTA KRAKOWA
Z DNIA 7 lutego 2008 roku

w sprawie zmiany zarządzenia Nr 243/2007 Prezydenta Miasta Krakowa z dnia 7 lutego 2007 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Urzędu Miasta Krakowa.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142 poz. 1591 z późn. zm.), § 10 zarządzenia Nr 18/2007 Prezydenta Miasta Krakowa z dnia 3 stycznia 2007 r. w sprawie Regulaminu Organizacyjnego Urzędu Miasta Krakowa (tekst jednolity zarządzenie Nr 5/2008 Prezydenta Miasta Krakowa z dnia 2 stycznia 2008 r. z późn. zm.), art. 36. ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (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) zarządza się, co następuje:

§ 1

W zarządzeniu Nr 243/2007 Prezydenta Miasta Krakowa z dnia 7 lutego 2007 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Urzędu Miasta Krakowa wprowadza się następujące zmiany:

- Pkt 7 otrzymuje brzmienie:

„7. Powołanie osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji w UMK.

1. W celu sprawnego zarządzania przetwarzaniem i bezpieczeństwem informacji, ustanawia się następujące funkcje:
    a. Funkcję **Głównego Administratora Informacji**, podległego bezpośrednio Prezydentowi Miasta Krakowa, upoważnionego do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych. Pełnienie tej funkcji powierza się Dyrektorowi Magistratu, który wykonuje ją przy pomocy Administratora Informacji przetwarzanych w SI, Administratora Informacji przetwarzanych poza SI oraz Administratora Bezpieczeństwa Informacji.
    b. Funkcję **Administratora Informacji przetwarzanych w SI**, podległego bezpośrednio Dyrektorowi Magistratu, upoważnionego do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych **w stosunku do danych osobowych przetwarzanych w Systemie**

Informatycznym UMK. Pełnienie funkcji Administratora Informacji przetwarzanych w SI powierza się Dyrektorowi Wydziału Informatyki.

c. Funkcję **Administratora Informacji przetwarzanych poza SI**, podległego bezpośrednio Dyrektorowi Magistratu, upoważnionego do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych **w stosunku do danych osobowych przetwarzanych poza SI**. Pełnienie funkcji Administratora Informacji przetwarzanych poza SI powierza się Z - cy Dyrektora Wydziału Organizacji i Nadzoru ds. Organizacyjnych.
d. Funkcję **Administratora Bezpieczeństwa Informacji,** podległego bezpośrednio Dyrektorowi Magistratu.

2. Administrator Informacji przetwarzanych w SI jest odpowiedzialny za określenie celu i środków przetwarzania informacji chronionych w SI UMK. W tym:
    a. Określenie, jakiego rodzaju informacje są przetwarzane w SI UMK.
    b. Ustalenie podziału informacji (określenie, czy jest to informacja chroniona).
    c. Określenie narzędzi, metod, miejsca i czasu przetwarzania informacji w SI UMK.
    d. Ustalenie własności informacji przetwarzanych w SI UMK.
    e. Przyznawanie dostępu do SI UMK.
    f. Nadzór na przestrzeganiem zasad bezpieczeństwa informacji przetwarzanych w SI UMK.
    g. Określenie zasad i opracowanie procedur bezpieczeństwa informacji chronionych przetwarzanych w SI UMK.
    h. Przygotowanie Polityki Bezpieczeństwa Systemu Informatycznego UMK oraz jej okresowe aktualizowanie.

3. Administrator Informacji przetwarzanych poza SI jest odpowiedzialny za określenie celów i środków przetwarzania informacji, a w szczególności danych osobowych, we wszystkich systemach w UMK poza Systemem Informatycznym UMK. W tym:
    a. Określenie, jakiego rodzaju informacje są przetwarzane w UMK poza Systemem Informatycznym.
    b. Ustalenie podziału informacji (określenie, czy jest to informacja chroniona).
    c. Określenie narzędzi, metod, miejsca i czasu przetwarzania informacji poza SI UMK.
    d. Ustalenie własności informacji przetwarzanych poza SI UMK.
    e. Określenie zasad bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK.
    f. Określenie zasad i opracowanie procedur bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK.
    g. Przygotowanie Polityki Bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK oraz jej okresowe aktualizowanie.

4. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za:
    a. Nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych w UMK.
    b. Przeprowadzanie okresowych kontroli bezpieczeństwa danych osobowych w UMK.
    c. Wydawanie upoważnień do przetwarzania danych osobowych oraz ich ewidencjonowanie.

d. Opracowanie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz jego aktualizacja.
e. Opracowanie wykazu zbiorów danych osobowych wraz ze wskazaniem programów służących do ich przetwarzania oraz jego aktualizacja.
f. Opis struktur zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi w obrębie zbioru danych oraz jego aktualizacja.
g. Opis sposobu przepływu danych osobowych pomiędzy poszczególnymi systemami w obrębie zbioru danych oraz jego aktualizacja.
h. Przygotowywanie projektów pełnomocnictw imiennych administratorów informacji.
i. Zatwierdzanie, modyfikowanie i akceptację przed przedłożeniem do podpisu Prezydentowi lub Dyrektorowi Magistratu proponowanych zmian zasad i procedur bezpieczeństwa przygotowywanych w UMK.
j. Opracowanie systemu szkoleń z zakresu bezpieczeństwa informacji oraz nadzór nad ich przeprowadzaniem.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Krakowa
/ - /