Zarządzenie Nr 423/2008

Burmistrza Nidzicy

z dnia 02 czerwca 2008 r.

w sprawie wyznaczenia administratora bezpieczeństwa informacji w Urzędzie Miejskim w Nidzicy oraz określenia jego zadań.

Na podstawie art. 31 oraz art. 33 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.), w związku z art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) Burmistrz Nidzicy zarządza, co następuje:

§ 1

Wyznacza się Pana Mariusza Dobrowolskiego na administratora bezpieczeństwa informacji w Urzędzie Miejskim Nidzicy.

§ 2

Ustala się zakres zadań administratora bezpieczeństwa informacji w Urzędzie Miejskiego w Nidzicy, w brzmieniu załącznika do zarządzenia.

§ 3

Wykonanie zarządzenia powierza Burmistrzowi Nidzicy.

§ 4

Traci moc zarządzenie nr 25/2005 Burmistrza Nidzicy – administratora Danych Osobowych z dnia 30 grudnia 2005 r. w sprawie wyznaczenia administratora bezpieczeństwa informacji.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Dariusz Szypulski

Załącznik
do Zarządzenia nr 423/2008
Burmistrza Nidzicy
z dnia 02 czerwca 2008 r.

Zakres zadań i uprawnienia administratora bezpieczeństwa informacji w Urzędzie Miejskim w Nidzicy

I. Administrator bezpieczeństwa informacji – zwany dalej ABI, jest pracownikiem Urzędu Miejskiego w Nidzicy i wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnienia nadanego przez Administratora Danych Osobowych.

II. Celem działania ABI jest nadzorowanie i kontrolowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Nidzicy. Zadaniem ABI jest realizacja przedsięwzięć określonych art. 36 ust. 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.), a w szczególności nadzorowanie i kontrolowanie:

1) stosowania środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednich do zagrożeń oraz kategorii danych,

2) zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym lub zabraniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem,

3) przetwarzania danych osobowych zgodnie z przepisami w/w ustawy.

III. ABI realizując swoje zadania współpracuje z administratorem systemu informatycznego (ASI). Do szczegółowych czynności ABI zaliczyć można:

1) nadzorowanie i kontrolowanie przestrzegania zasad:

a) przetwarzania danych osobowych przez użytkowników zgodnie z zakresem nadanego im upoważnienia;
b) prowadzenia dokumentacji przetwarzania danych osobowych;
c) stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania;
d) ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń;
e) wyposażenia oraz zabezpieczenia pomieszczeń, w których przechowuje się dane sensytywne i kopie zapasowe zbiorów;
f) rejestracji zbiorów w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GIODO) lub zmian przetwarzania danych osobowych,

2) realizowanie zadań w zakresie:

a) rozpatrywania skarg i wniosków dotyczących przetwarzania i ochrony danych;
b) tworzenia projektów zarządzeń, instrukcji i wytycznych Administratora;
c) przygotowywania informacji w zakresie rejestracji zbiorów w GIODO lub zmian w przetwarzaniu danych;
d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych;
e) organizowania szkoleń z zakresu przetwarzania i ochrony danych osobowych;
f) odnotowywania i dokumentowania zmian w lokalizacjach obszarów przetwarzania danych;

g) wykonywania okresowych analiz zagrożeń bezpieczeństwa i ocen stanu ochrony danych osobowych przetwarzanych w obszarach.

IV. Wykonując swoje czynności ABI działa w imieniu Administratora Danych i posiada uprawnienia do:

1) wskazywania zastosowania odpowiednich zabezpieczeń technicznych i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych;
2) parafowania umów dotyczących udostępniania lub powierzania danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania w nich zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych;
3) wnioskowania o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych;
4) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa;
5) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.

BURMISTRZ

Dariusz Szypulski