ZARZĄDZENIE NR 12/2010
WÓJTA GMINY SŁUPIA JĘDRZEJOWSKA
Z DNIA 16 KWIETNIA 2010R.

w sprawie wykonywania ustawy o ochronie danych osobowych w Urzędzie Gminy Słupia.

Na podstawie art.33 ust 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tekst jednolity z 2001r. Dz.U. Nr 142, poz.1591 z późniejszymi zmianami) zarządza się, co następuje:

§ 1.

Zobowiązuje się Kierowników Referatów Urzędu oraz stanowiska pracy do wykonywania obowiązków administratora danych określonych w ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz.226) w zakresie przetwarzania zbiorów danych znajdujących się w dyspozycji Referatu, a w szczególności do:
- decydowania o środkach i celach przetwarzania danych osobowych,
- zabezpieczenia przed niepowołanym dostępem zbiory danych osobowych zawartych w kartotekach, księgach, wykazach i innych zbiorach ewidencyjnych,
- zabezpieczenia pomieszczeń, pomieszczeń, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
- wskazania użytkowników zbiorów danych osobowych.

§ 2.

Osoby, które zostały upoważnione do przetwarzania danych są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

§ 3.

1. Wyznacza się Pana Marcina Nowaka administratorem bezpieczeństwa informacji w systemie informacyjnym.
2. Upoważnia się administratora bezpieczeństwa informacji do podejmowania działań zabezpieczających system informacyjny przed niepowołanym dostępem do zgromadzonych w nim zbiorów danych osobowych.

§ 4.

Wprowadza się do stosowania w Urzędzie Gminy:
- instrukcje postępowania w sytuacji naruszenia ochrony danych w brzmieniu załącznika Nr 1
- instrukcje zarządzania systemem informatycznym zawierającym zbiory danych osobowych w brzmieniu załącznika Nr 2

§ 5.

Traci moc Zarządzenie Nr 4/2004 Wójta Gminy Słupia Jędrzejowska z dnia 10 lutego 2004r. w sprawie wykonywania ustawy o ochronie danych osobowych w Urzędzie Gminy Słupia.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy
Słupia Jędrzejowska
Janusz Grabek

Załącznik Nr 1 do
Zarządzenia Wójta Gminy
z dnia 16 kwietnia 2010r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

1. Osoby zatrudnione przy przetwarzaniu danych osobowych w przypadki stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub podejrzenia , że takie naruszenie nastąpiło zobowiązane są:
   a) zabezpieczyć pomieszczenie, w którym znajduje się urządzenie informatyczne (komputer) przed dostępem osób trzecich,
   b) zawiadomić o naruszeniu lub podejrzeniu, że nastąpiło naruszenie zabezpieczenia systemu informatycznego administratora bezpieczeństwa informacji.
2. Administrator bezpieczeństwa informacji:
   a) ustala, czy ostatni użytkownik systemu działał zgodnie z procedurą korzystania ze zbioru danych osobowych, a w szczególności czy prawidłowo zabezpieczył system po zakończeniu pracy,
   b) opisuje stan urządzenia, dowody lub okoliczności wskazujące na naruszenie lub podejrzenie, że takie naruszenia zabezpieczenia systemu informatycznego.
   c) zawiadamia Wójta o fakcie naruszenia zabezpieczenia systemu informatycznego lub podejrzeniu, że takie naruszenie nastąpiło i przekazuje mu treść dokonanych ustaleń.
3. W przypadku podejrzenia popełnienia przestępstwa Wójt powiadamia o dokonanym naruszeniu zabezpieczenia systemu informatycznego albo podejrzeniu, że takie naruszenie nastąpiło, organy ścigania.

Załącznik Nr 2 do
Zarządzenia Wójta Gminy
z dnia 16 kwietnia 2010r.

Instrukcja zarządzania systemem informatycznym zawierającym zbiory danych osobowych:

1. Kierownicy Referatów, wykonujący obowiązki administratora danych osobowych przekazują administratorowi bezpieczeństwa informacji wykaz pracowników, wykonujących zadania polegające na przetwarzaniu danych osobowych w systemie informatycznym.
2. O zmianie pracownika na stanowisku, o którym wyżej, Kierownik Referatu niezwłocznie zawiadamia administratora bezpieczeństwa informacji.
3. Administrator bezpieczeństwa informacjo przydziela identyfikator i hasła dostępu dla użytkowników zbiorów danych osobowych (osób zatrudnionych przy przetwarzaniu danych osobowych).
4. Rejestr użytkowników, ich identyfikatorów i przydzielonych haseł prowadzi administrator bezpieczeństwa informacji. Treść rejestru stanowi tajemnicę służbową.
5. Hasło dostępu użytkownika administrator bezpieczeństwa informacji zmienia raz w miesiącu.
6. Hasła użytkownika umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie terminu ważności.
7. Identyfikator użytkownika nie ulega zmianie. Po wyrejestrowani użytkownika z systemu informatycznego, identyfikator nie powinien być przydzielony innej osobie.
8. Kopie awaryjne zbiorów danych osobowych tworzy się w dwóch egzemplarzach przechowywanych oddzielnie.
9. Sprawdzenie obecności wirusów komputerowych raz w tygodniu dokonuje administrator bezpieczeństwa informacji.
10. Nośniki informacji (dyskietki, płyty CD, dyski, wydruki itp.) przechowuje administrator bezpieczeństwa systemu. Po ustaniu okresu użyteczności informacje zawarte na nośnikach informacji lub wydrukach podlegają bezzwłocznemu usunięciu. Nośniki i wydruki zawierające informacje niejawne przechowywane są zgodnie z zasadami określonymi w ustawie o ochronie informacji niejawnych.
11. Przeglądów zbiorów danych osobowych , ich aktualizacji, dokonuje użytkownik systemu.
12. Przeglądów i konserwacji systemów informatycznych dokonuje administrator bezpieczeństwa informacji.
13. Komunikacja w sieci komputerowej Urzędu nie uprawnia do przetwarzania danych osobowych bez zgody administratora danych.
14. Udostępnienie danych osobowych dla podmiotów zewnętrznych poprzez komunikację w sieci komputerowej dopuszczalne jest po spełnieniu warunków określonych ustawą o ochronie danych osobowych. Użytkownik systemu odnotowuje fakt udostępnienia danych osobowych przez określenie kiedy, komu i w jakim zakresie zostały one udostępnione.
15. Ustala się następującą procedurę rozpoczęcia i zakończenia pracy przez użytkownika:
    a) praca na komputerze winna się odbywać w godzinach 8.00-15.00,
    b) podczas pracy na komputerze nie wolno pozostawiać urządzenia włączonego bez nadzoru,
    c) praca z programem ogranicza się do osób uprawnionych do posługiwania się nim.