Zarządzenie Nr 5/2009
STAROSTY PIŃCZOWSKIEGO
z dnia 2 lutego 2009 r.

w sprawie ochrony danych osobowych Starostwa Powiatowego w Pińczowie i powołania Administratora Bezpieczeństwa Informacji

Na podstawie art. 3 i art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. Nr 101 poz. 926 z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 z późn. zm.) zarządzam co następuje:

§ 1

Przetwarzanie danych osobowych pracowników i petentów Starostwa powiatowego w Pińczowie służy do realizacji zadań wynikających z art. 4 ustawy o samorządzie powiatowym z dnia 5 czerwca 1998 R. (Dz. U. Nr 142 poz. 1593 z późn. zm.)

§ 2

1. Administratorem danych w Starostwie Powiatowym w' Pińczowie w rozumieniu ustawy o ochronie danych osobowych jest Starosta.
2. Obowiązki wynikające z ustawy o ochronie danych osobowych Starosta powierza kierownikom wydziałów Starostwa (zwanych dalej lokalnymi administratorami danych osobowych) - w zakresie podległych im pracowników.

§ 3

1. Zgodnie z wymogami art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. Nr 101 poz. 926 z późn. zm.) wyznaczam Z-cę Kierownika Wydziału Organizacyjnego i Spraw Obywatelskich tut. Starostwa Pana Michała Klamińskiego do pełnienia

funkcji „administratora bezpieczeństwa informacji", odpowiedzialnego za bezpieczeństwo danych osobowych w systemach informatycznych Starostwa Powiatowego w Pińczowie.

2. Administrator bezpieczeństwa informacji realizuje zadania wynikające z Rozporządzenia MSWiA przy pomocy:
   a. pracownika ds. kadr
   b. głównego specjalisty ds. informatyki – administratora systemów informatycznych Starostwa
   c. lokalnych administratorów danych osobowych – Kierowników Wydziałów Starostwa Powiatowego w Pińczowie

§ 4

1. Zobowiązuje się administratora bezpieczeństwa informacji do:
   a. Prowadzenia ewidencji baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Starostwie powiatowym w Pińczowie, zgodnie z załącznikiem Nr 1 do niniejszego zarządzenia,
   b. Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów, zgodnie z załącznikiem Nr 2 do niniejszego zarządzenia,
   c. Prowadzenia ewidencji miejsc przetwarzania danych osobowych i sposobu ich zabezpieczenia, zgodnie z załącznikiem Nr 3 do niniejszego zarządzenia,
2. Zobowiązuje się pracownika ds. kadr do uzupełnienia akt osobowych pracowników zatrudnionych przy przetwarzaniu danych osobowych o oświadczenia, z których wynika, że zapoznali się z przepisami obowiązującymi w tym zakresie.

Udostępnianie danych osobowych pracowników i petentów do celów innych niż określone w § 1 niniejszego zarządzenia, odbywa się wyłącznie za pośrednictwem pracownika ds. kadr lub lokalnych administratorów danych osobowych w przypadku petentów, po uprzednim uzyskaniu zgody Starosty lub Wicestarosty.

§ 5

1. Zgodnie z wymogami § 11 ust. 1 Rozporządzenia MSWiA wprowadza się do stosowania Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, stanowiącą załącznik Nr 4 do niniejszego zarządzenia.
2. Zgodnie z wymogami § 6 ust. 1 Rozporządzenia MSWiA wprowadza się do stosowania Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, stanowiącą załącznik Nr 5 do niniejszego zarządzenia.

§ 6

Lokalni administratorzy danych osobowych zobowiązani są do przestrzegania wszelkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określenie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. zapoznanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
3. wykonanie zaleceń administratora bezpieczeństwa informacji i głównego specjalisty ds. informatyki – administratora systemów informatycznych starostwa w zakresie ochrony danych osobowych w funkcjonujących w podległym im wydziale systemach informatycznych,
4. przekazywanie na bieżąco do administratora bezpieczeństwa informacji aktualnych danych w zakresie wykazu baz danych w systemach informatycznych, w których przetwarzane są dane osobowe, zgodnie z załącznikiem Nr 1 do niniejszego zarządzenia, listy osób biorących udział przy przetwarzaniu danych osobowych i ich identyfikatorów, zgodnie z załącznikiem Nr 2 do niniejszego zarządzenia oraz lokalizacji pomieszczeń w których te dane są przetwarzane, zgodnie z załącznikiem Nr 3 do niniejszego zarządzenia, w przypadku zaistnienia jakichkolwiek zmian tych danych,
5. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, będącej załącznikiem Nr 4 do niniejszego zarządzenia,
6. działanie zgodnie z instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych, będącą załącznikiem Nr 5 do niniejszego zarządzenia,
7. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych w podległym im wydziałach.

§ 7

Osoby nie przestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom przewidzianym w rozdziale 8 ustawy o ochronie danych osobowych.

§ 8

Zobowiązuje się lokalnych administratorów danych osobowych w terminie 30 dni od wejścia w życie zarządzenia do:

1. zgodnie z załącznikiem Nr 1 przygotowanie i przesłanie do administratora bezpieczeństwa informacji ewidencji baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
2. zgodnie z załącznikiem Nr 2 przygotowanie i przesłanie do administratora bezpieczeństwa informacji listy osób zatrudnionych przy przetwarzaniu danych osobowych i ich identyfikatorów,
3. zgodnie z załącznikiem Nr 3 przygotowanie i przesłanie do administratora bezpieczeństwa informacji wykazu miejsc, w których ma miejsce przetwarzanie danych osobowych, w podległych wydziałach.

§ 9

Traci moc Zarządzenie Nr 18/2008 Starosty Pińczowskiego z dnia 26 listopada 2008 roku w sprawie Administratora Bezpieczeństwa Informacji Starostwa Powiatowego w Pińczowie

§ 10

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
dr inż. Andrzej Kozera

opr.

Załącznik nr 1
do zarządzenia nr 5/2009
z dnia 02 lutego 2009r.

.....
Nazwa wydziału/jednostki organizacyjnej

Wykaz baz danych w systemach informatycznych w których przetwarzane są dane osobowe w Starostwie Powiatowym w Pińczowie

Lp.	Nazwa bazy danych[1]	Wersja bazy danych	Forma bazy danych/System operacyjny serwera[2]	Sposób zabezpieczenia informatycznego[3]	Zawiera także dane osób spoza UG (T/N)	Baza danych chroniona przez UPS (T/N)	Liczba miejsc przetwarzania i liczba porządkowa załączników nr 3

[1]nazwa zwyczajowa lub własna, np.księgowość, kadry, itp.
[2]np. plik Excela/Windows 2000, lub baza MySQL/Mandrake 9.0
[3]np. (I) indywidualne hasło dostępu do bazy danych, (S) szyfrowanie bazy danych, (F) wydzielonafizycznie sieć
[4]np. kontrola dostępu

Załącznik nr 2
do zarządzenia nr 5/2009
z dnia 02 lutego 2009r.

.....
Nazwa wydziału/jednostki organizacyjnej

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów

Lp.	Nazwa bazy danych [1]	Nazwisko i imię użytkownika	Nazwa identyfika-tora	Rodzaj uprawnień[2]	Data zarejest.	Data wyrejest.	Lokali-zacja [3]	Uwagi

[1]Nazwa bazy danych z załącznika nr 1
[2]Skróty stosowane do określenia uprawnień
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych
Uwaga: w przypadku praw ograniczonych do określonej części bazy danych należy ograniczenie to podać w polu Uwagi
[3]należy podać liczbę porządkową zgodnie z załącznikiem nr 3

Dane aktualne na dzień:...../...../.....

Sporządził:.....

Załącznik nr 3
do zarządzenia nr 5/2009
z dnia 02 lutego 2009r.

.....
Nazwa wydziału/jednostki organizacyjnej

Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych w Starostwie Powiatowym w Pińczowie

UWAGA: do każdej lokalizacji należy dołączyć szkic sytuacyjny określający położenie stanowisk komputerowych w pomieszczeniu, z zaznaczeniem strefy ochronnej do której nie mają dostępu osoby nieupoważnione, drzwi wejściowe, okna oraz zabezpieczenia fizyczne.

Lp.	Nazwa bazy danych[1]	Lokalizacja (adres)	Nr pokoju /piętro	Funkcja lokalizacji [2]	Zabezpieczenie fizyczne [3]

[1]nazwa bazy danych z załącznika nr 1
[2](S) - serwer, (K) – miejsce przechowywania kopii bezpieczeństwa, Z – pomieszczenie w którym wykonywane są kopie bezpieczeństwa, U – pomieszczenie osób wprowadzających dane, A – pomieszczenie administratora bazy danych
[3](K) – kraty w oknach, (A) – alarm, (W) – wzmocnione drzwi

Załącznik nr 4
do zarządzenia nr 5/2009
z dnia 02 lutego 2009r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

1. Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Pińczowie oraz stanowi podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych funkcjonujących w starostwie.

2. Administrator bezpieczeństwa informacji Starostwa Powiatowego
   a - czuwa nad wdrażaniem niniejszej instrukcji w systemach informatycznych Starostwa Powiatowego w których przetwarzane są dane osobowe oraz dba o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych starostwa
   b - określa strategię zabezpieczania systemów informatycznych starostwa
   c - identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych starostwa
   d - określa potrzeby w zakresie zabezpieczenia systemów informatycznych w których przetwarzane są dane osobowe
   e - monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz ich przetwarzania

3.Lokalni administratorzy danych osobowych stwarzają właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych w podległych im jednostkach, a w szczególności:
   a - stosują się do zaleceń administratora bezpieczeństwa informacji (lub - uwzględniają w miarę możliwości finansowo- lokalowych zalecenia administratora bezpieczeństwa informacji) w zakresie:
   - lokalizacji pomieszczeń w których przetwarzane są dane osobowe
   - lokalizacji pomieszczeń w których przechowywane są ko pie awaryjne zbiorów danych osobowych
   - instalowania krat i systemów alarmowych adekwatnych do zagrożenia systemów informatycznych
   - zakupu systemów operacyjnych, baz danych, oprogramowania antywirusowego oraz systemów kryptograficznych podnoszących bezpieczeństwo danych osobowych oraz gwarantujących spełnienie wymogów określonych ustawą
   - zakupu pamięci masowych, streamerów oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych

- właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej służącej do przetwarzania danych osobowych w systemach informatycznych w celu wyeliminowania niebezpieczeństwa podsłuchu lub zniszczenia infrastruktury sieciowej
- zakupu niszczarek do dokumentów do pomieszczeń w których generowane są wydruki zawierające dane osobowe
- zakupu szaf pancernych do przechowywania kopii zapasowych danych osobowych z systemów informatycznych

b - w przypadku systemów informatycznych działających w środowisku sieciowym:
- dokonują wyboru lub migracji do technologii minimalizującej zagrożenie uzyskania dostępu do sieci osobom nieupoważnionym
- zakupują oprogramowanie umożliwiające rejestrowanie identyfikatorów i czas logowania użytkowników sieci
- nadzorują proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych

c - zabezpieczają budynki oraz pomieszczenia w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych, a w szczególności:
- wprowadzają i nadzorują bieżącą aktualizację listy osób upoważnionych do pobierania kluczy do pomieszczeń w których przetwarzane są dane osobowe
- wprowadzają ewidencję osób pobierających klucz do pomieszczeń w których przetwarzane są dane osobowe zawierającą m.in. czas pobierania i zdawania kluczy
- określają tryb szkolenia osób sprzątających pomieszczenia w których przetwarzane są dane osobowe w systemach informatycznych uwzględniający specyfikę konserwacji systemów komputerowych

d - określają zasady i ewidencję wykonywania czynności serwisowych w systemach informatycznych w podległych jednostkach w celu wyeliminowania
- możliwości wykonania kopii danych osobowych przez osoby nieupoważnione,
- przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną
- podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera cechy ukryte

4.1 Administrator sieci komputerowej opracowuje i na bieżąco uaktualnią szczegółowe instrukcje zarządzania systemami informatycznymi w podległych mu systemach informatycznych, które powinny zawierać w szczególności

a - sposób przydziału haseł dla użytkowników poszczególnych syste mów informatycznych i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności

b - określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności

c - procedury rozpoczęcia i zakończenia pracy

d - metody i częstotliwość wykonywania kopii awaryjnych

e - metody i częstotliwość sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metodę ich usuwania

f - sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków

g - sposób postępowania w zakresie komunikacji w sieci komputerowej

4.2 Administrator sieci komputerowej zobowiązany jest do:

a - wykonywania poleceń administratora bezpieczeństwa informacji Starostwa Powiatowego w zakresie zarządzania podległymi systemami informatycznymi

b - czuwania nad właściwym eksploatowaniem podległych im systemów informatycznych

c - prowadzenia, uaktualniania na bieżąco oraz przesyłania administratorowi bezpieczeństwa informacji Starostwa Powiatowego, danych w zakresie:

- listy osób biorących udział przy przetwarzaniu danych osobowych
- lokalizacji pomieszczeń w których te dane są przetwarzane, w przypadku zaistnienia jakichkolwiek zmian tych danych
- rodzaju systemów informatycznych funkcjonujących w zakresie ich działania
- listy identyfikatorów osób biorących udział przy przetwarzaniu danych osobowych w podległych mu systemach informatycznych
- czynności serwisowych wykonywanych w podległych systemach informatycznych
- zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytych wirusów, koni trojańskich itp. oprogramowania nielegalnego lub zainstalowanego bez upoważnienia
- awarii systemu informatycznego lub jego nieprawidłowego działania
- stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną
- awarii zasilania

d - kontrolowania i zabezpieczenia prawidłowości przebiegu czynności serwisowych w podległych systemach informatycznych, przy czym urządzenia, dyski lub inne nośniki zawierające dane osobowe, pozbawia przed naprawą zapisu tych danych lub nadzoruje ich naprawę

e - pozbawiania zapisu danych osobowych z tych nośników, które przeznaczone są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych

f - pozbawiania zapisu danych osobowych lub uszkadzania w sposób uniemożliwiający odczytanie tych nośników, które przeznaczone są do likwidacji

g - instalowania zabezpieczeń w podległych systemach informatycznych wynikających z zaleceń administratora bezpieczeństwa informacji Starostwa Powiatowego

h - zgłaszania wydziałowym administratorom danych oraz administratorowi bezpieczeństwa informacji Starostwa Powiatowego potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych

i) - postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych

j) - okresowego sprawdzania kopii awaryjnych pod kątem prawidłowości ich wykonania oraz ich dalszej przydatności do odtworzenia w przypadku awarii

k) - znajomości oraz posiadania dokumentacji funkcji poszczególnych systemów informatycznych ze szczególnym uwzględnieniem procedur:

- dostępu i modyfikowania do danych osobowych
- zarządzania identyfikatorami i hasłami użytkowników
- wykonywania kopii awaryjnych oraz odtwarzania danych z tych kopii
- generowania wydruków danych osobowych
- dostępu do plików rejestrujących identyfikatory oraz czas logowania użytkowników

5. Administrator poszczególnych systemów informatycznych służących do przetwarzania danych osobowych odpowiada za ich bieżącą eksploatację, a w szczególności za:

a - wszystkie czynności związane z ich funkcjonowaniem i modernizacją

b - rejestrowanie i wyrejestrowywanie z systemu użytkowników oraz projektantów i programistów w czasie instalowania systemu oraz jego modyfikacji

c - przydzielanie uprawnień do poszczególnych funkcji systemu oraz określenie trybu i częstotliwości zmiany haseł

d - procedury wykonywania kopii awaryjnych, określenie ich częstotliwości, zmianę nośników oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i likwidację

e - lokalizację sprzętu komputerowego, ustawienie monitorów i drukarek uniemożliwiające wgląd w dane osobom nieupoważnionym lub kradzież wymiennych nośników danych

f - postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych

Załącznik nr 5
do zarządzenia nr 5/2009
z dnia 02 lutego 2009r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego, lub
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy pracownik Starostwa Powiatowego, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym Starostwa Powiatowego zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego, lokalnego administratora danych osobowych lub w przypadku ich nieobecności administratora bezpieczeństwa informacji Starostwa Powiatowego.

Administrator bazy danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1. zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
2. jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
3. przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
4. podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
   a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

c)zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

5.szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

6.przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

- Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
- Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
- Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

Administrator bazy danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych, w porozumieniu z właściwym lokalnym administratorem danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje lokalnemu administratorowi danych oraz administratorowi bezpieczeństwa informacji Starostwa Powiatowego.

Administrator bezpieczeństwa informacji w Starostwie Powiatowym przeprowadza analizę raportów pochodzących od wydziałowych administratorów bezpieczeństwa informacji i uwzględnia je w opracowywaniu corocznego raportu dla administratora danych w Starostwie Powiatowym.