Załącznik nr 4
Do Zarządzenia nr ....25.../.2003.
Starosty Poznańskiego
Z dnia 22.09.2003r.

Regulamin przetwarzania danych osobowych

Starostwo Powiatowe w Poznaniu

STAROSTA POZNAŃSKI
Jan Grabkowski
Starosta

Opracował:

Marek Jóźwiak
Piotr Siwczak

Rozdział I

Przepisy ogólne

§ 1

1) Na podstawie ustawy z dnia 29 sierpnia 1998 r. o ochronie danych osobowych (Dz. U. Nr 133. poz. 883) ustanawia się regulamin przetwarzania danych osobowych.
2) Regulamin przetwarzania danych osobowych ustala zasady przetwarzania i ochrony danych osobowych w Starostwie Powiatowym w Poznaniu oraz określa obowiązki pracodawcy związane z ochroną danych osobowych.

§ 2

Przez użyte w Regulaminie określenie:

- pracodawca - rozumie się Starostwo Powiatowe w Poznaniu (STAROSTĘ);
- dane osobowe - rozumie się każdą informację dotyczącą osoby: fizycznej. pozwalającą na określenie tożsamości tej osoby;
- przetwarzanie danych osobowych - rozumie się jakiekolwiek operacje wykonywane na danych osobowych. takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. a zwłaszcza te, które dokonuje się w systemach informatycznych;
- administrator bezpieczeństwa informacji - rozumie się wyznaczoną przez pracodawcę osobę odpowiedzialną za bezpieczeństwo danych osobowych;
- pracownik - rozumie się osobę zatrudnioną w Starostwie Powiatowym w Poznaniu;
- obszar przetwarzania danych osobowych - rozumie się budynki. pomieszczenia lub części pomieszczeń stanowiące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego;
- naruszenie ochrony danych osobowych - rozumie się nielegalne ujawnienie, pozyskanie, nieuzasadnioną modyfikację lub zniszczenie danych osobowych, niepowołany dostęp.
- system informatyczny - rozumie się system informatyczny oraz urządzenia wchodzące w jego skład i służące do przetwarzania danych osobowych.

Rozdział II

Administrator bezpieczeństwa informacji

§ 3

Starosta ustanawia administratora bezpieczeństwa informacji w osobie ..... odpowiedzialnego za bezpieczeństwo danych osobowych, do którego obowiązków należą czynności określone niniejszym regulaminem.

Rozdział III

Wprowadzenie polityki bezpieczeństwa systemu informatycznego

§4

Obsługa systemu informatycznego:

1) Obsługiwać system informatyczny, mogą wyłącznie pracownicy upoważnieni przez Starostę i zaznajomieni z przepisami dotyczącymi ochrony danych osobowych.
2) Pracownicy wskazani w ust 1 ponoszą odpowiedzialność, w zakresie wynikającym z prawa pracy, za szkody spowodowane naruszeniem ochrony danych osobowych - w stopniu odpowiednim do ich zadań przy przetwarzaniu danych osobowych.
3) Starosta (pełnomocnik ds. ochrony informacji niejawnych i danych osobowych) prowadzi ewidencję pracowników upoważnionych przez niego do obsługi systemu informatycznego.

§ 5

1) W przypadku stwierdzenia naruszenia ochrony danych osobowych pracownicy wskazani w § 4 ust 1 oraz inni użytkownicy systemu informatycznego mają obowiązek wstrzymania się z jakimikolwiek czynnościami dokonywanymi w systemie informatycznym, poza jego zabezpieczeniem przed dostępem osób nieuprawnionych, oraz niezwłocznego poinformowania administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę o fakcie naruszenia.
2) Postanowienia ust1 stosuje się również w przypadku, gdy stan urządzeń, zawartość zbioru danych osobowych, sposób działania systemu informatycznego lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenia ochrony danych osobowych.

§ 6

1) Pomieszczenia:
    a. Zarządu Powiatu
    b. Skarbnika
    c. Biura Rady Powiatu
    d. Gabinet Starosty
    e. Wydziału Organizacji i Kadr
    f. Wydziału Finansów
    g. Wydziału Administracyjnego (za wyjątkiem pomieszczenia kierowców – pok. nr 2)
    h. Wydziału Komunikacji i Transportu
    i. Wydziału Administracji Architektoniczno – Budowlanej
    j. Wydziału Integracji Europejskiej, Promocji i Kultury
    k. Wydziału Nieruchomości
    l. Wydziału Ochrony Środowiska, Rolnictwa i Leśnictwa
    m. Zespołu Radców Prawnych
    n. Zespołu Kontroli
    o. Zespołu Spraw Obywatelskich i Zarządzania Kryzysowego
    p. Zespołu Edukacji
    q. Zespołu Inwestycji i Remontów
    r. Zespołu Zdrowia, Polityki Społecznej i Osób Niepełnosprawnych
    s. Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności
    t. Powiatowego Rzecznika Konsumentów
    u. Pełnomocnika ds. Ochrony Informacji Niejawnych

    znajdujące się w budynku Starostwa Powiatowego w Poznaniu przy ulicy Jackowskiego 18 (segmenty: A, B, C i D) stanowią obszar przetwarzania

danych osobowych.
2) Przebywanie osób nieuprawnionych do dostępu do danych osobowych wewnątrz obszaru przetwarzania danych osobowych jest dopuszczalne tylko w obecności pracownika wskazanego w § 4 ust 1 i za zgodą administratora bezpieczeństwa informacji lub innej upoważnionej przez niego osoby.
3) Pomieszczenia określone w ust. 1 powinny być zamykane na czas nieobecności w nich pracowników wskazanych w § 4 ust. 1, w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.

§ 7

1) Osoba korzystająca z przenośnego komputera, służącego do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem przetwarzania danych osobowych, w celu zapobieżenia naruszenia ochrony danych osobowych.
2) Osoba wskazana w ust 1 ma obowiązek zabezpieczyć dostęp do komputera hasłem oraz nie zezwalać na używanie komputera osobom nieupoważnionym przez pracodawcę do dostępu do danych osobowych.

§ 8

1) Administrator bezpieczeństwa informacji przydziela każdemu użytkownikowi systemu informatycznego osobisty identyfikator dający, w połączeniu z hasłem ustalanym przez użytkownika, dostęp do systemu informatycznego.
2) Hasło dostępu poszczególnego użytkownika podlega zmianie nie rzadziej niż raz na miesiąc. Długość hasła wynosi nie mniej niż 5 znaków. Wprowadzane hasła są unikalne.
3) Identyfikator każdego użytkownika zostaje wpisany do ewidencji wskazanej w § 4 ust. 3 wraz z imieniem i nazwiskiem użytkownika oraz podlega rejestracji w systemie informatycznym,
4) Identyfikator użytkownika nie podlega zmianie, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
5) Użytkownik systemu informatycznego nie może udostępniać innym osobom własnego hasła lub identyfikatora w celu uzyskania dostępu do systemu informatycznego,
6) Każdy użytkownik systemu informatycznego ma obowiązek zachować w tajemnicy indywidualne hasło oraz identyfikator, w szczególności przed osobami nieuprawnionymi do korzystania z systemu informatycznego.
7) Administrator bezpieczeństwa informacji prowadzi listę użytkowników systemu informatycznego służącego do przetwarzania danych osobowych.

§ 9

Administrator bezpieczeństwa informacji jest odpowiedzialny za nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkownika i kontroli dostępu do systemu informatycznego,

§ 10

Użytkownicy systemu informatycznego mają obowiązek stosować następującą procedurę rozpoczęcia, prowadzenia i zakończenia pracy w systemie:
a) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może nastąpić wyłącznie po podaniu identyfikatora i hasła danego użytkownika,

b) w przypadku jakiejkolwiek przerwy w pracy w systemie informatycznym i opuszczenia stanowiska, użytkownik ma obowiązek zamknąć system w sposób uniemożliwiający innym osobom dostęp do systemu informatycznego,
c) każdy użytkownik systemu informatycznego ma obowiązek korzystania z systemu informatycznego w sposób uniemożliwiający osobom nieuprawnionym zapoznanie się z danymi osobowymi znajdującymi się w systemie informatycznym,
d) po zakończeniu pracy użytkownik ma obowiązek zamknąć system w sposób uniemożliwiający innym osobom dostęp do systemu informatycznego,

§ 11

1) Administrator bezpieczeństwa informacji ma obowiązek sporządzania kopii awaryjnych poprzez skopiowanie danych osobowych na kasetę, płytę CD, inny dysk twardy nie rzadziej niż co 4 tygodnie,

2) Kopie awaryjne wskazane w ust. 1 przechowywane są w następujących pomieszczeniach:
   a. Pomieszczenia Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności (segment D – parter)
   b. Serwerownia (segment B – pok. 7)
   c. Pomieszczenia Wydziału Komunikacji i Transportu (segment C – parter)

   nie mogą być przechowywane w pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

3) Administrator bezpieczeństwa informacji ma obowiązek dokonywać okresowego, nie rzadziej niż co 4 tygodnie, sprawdzenia kopii awaryjnych pod kątem ich przydatności do odtworzenia danych osobowych.

§ 12

1) Administrator bezpieczeństwa informacji ma obowiązek sprawdzania obecności wirusów w systemie informatycznym za pomocą odpowiednich programów antywirusowych nie rzadziej niż co 4 tygodnie.
2) W przypadku wykrycia wirusa, administrator bezpieczeństwa informacji ma obowiązek usunąć wirus przy zastosowaniu odpowiednich programów antywirusowych.

§ 13

1) Administrator bezpieczeństwa informacji ma obowiązek dokonywania okresowych, nie rzadziej niż co 3 miesiące, przeglądów i konserwacji systemu informatycznego,
2) Przed przystąpieniem do przeglądu lub konserwacji systemu informatycznego, administrator bezpieczeństwa informacji ma obowiązek sporządzenia kopii awaryjnych zgodnie z § 11 regulaminu.
3) Przeglądy i konserwacja systemu informatycznego mogą być wykonywane wyłącznie przez osoby upoważnione przez pracodawcę lub pod nadzorem administratora bezpieczeństwa informacji.
4) Przeglądy i konserwacje systemu informatycznego powinny być dokonywane w sposób uniemożliwiający naruszenie ochrony danych osobowych.

§ 14

1) Urządzenia, dyski lub inne nośniki informatyczne zawierające dane osobowe przeznaczone do likwidacji, pracownicy. wskazani w § 4 ust. 1 lub ich przełożeni, mają obowiązek pozbawić wcześniej zapisu tych danych, a w przypadku gdy nie jest

to możliwe. uszkodzić je w sposób uniemożliwiający ich odczytanie.
2) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do naprawy, pracownicy, wskazani w § 4 ust. 1, mają obowiązek pozbawić, o ile to możliwe, zapisu tych danych. bądź naprawa winna być dokonana pod nadzorem osoby upoważnionej przez pracodawcę.
3) Urządzenia, dyski lub inne nośniki informatyczne zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi nieuprawnionemu do otrzymania danych osobowych, pracownicy, wskazani w § 4 ust. 1 mają obowiązek pozbawić wcześniej zapisu tych danych.

§ 15

Wszelkie nośniki informacji zawierające dane osobowe oraz wydruki danych osobowych przechowywane są w pomieszczeniach wspomnianych w § 6 ust. 1.

§ 16

Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osób niepowołanych.

§ 17

Administrator bezpieczeństwa informacji ma obowiązek kontroli stanu zabezpieczenia pomieszczeń wskazanych w § 11 ust. 2 oraz § 15 przed dostępem do nich osób niepowołanych.

§ 18

Użytkownicy systemu informatycznego mają obowiązek zgłaszania administratorowi bezpieczeństwa informacji wszelkich stwierdzonych nieprawidłowości w funkcjonowaniu systemu informatycznego.

§ 19

Wszelkie osoby mające dostęp do danych osobowych mają obowiązek zachowania ich w tajemnicy.

Rozdział IV

Udostępnianie danych osobowych

§ 20

Każda osoba, której dane osobowe są przetwarzane w systemie informatycznym, ma prawo uzyskać na piśmie. w powszechnie zrozumiałej formie, treść tych danych oraz następujące informacje:
1) datę pierwszego wprowadzenia danych tej osoby,
2) źródło pochodzenia danych,
3) identyfikator użytkownika wprowadzającego dane,
4) jakim uprawnionym podmiotom, kiedy i w jakim zakresie dane zostały udostępnione,
5) dotyczące sprzeciwów osoby, której dane dotyczą, przeciwko przetwarzaniu danych.

Rozdział V

Postanowienia końcowe

§ 21

Postanowienia niniejszego regulaminu stosuje się odpowiednio do przetwarzania danych osobowych w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 22

W sprawach nie objętych niniejszym regulaminem mają zastosowanie przepisy ustawy o ochronie danych osobowych.

§ 23

Regulamin wchodzi w życie z dniem ogłoszenia.

Poznań,.....r.(data) 22.09.2003r.

STAROSTA POZNAŃSKI

Jan Grabkowski