Zarządzenie Nr 52/2007
Burmistrza Miasta i Gminy Piotrków Kujawski
z dnia 6 listopada 2007 r.

w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych" i „Instrukcji zarządzania systemem informatycznym do przetwarzania danych osobowych" w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim.

Na podstawie § 3 ust 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) zarządza się, co następuje:

§ 1

Wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim", zwaną dalej polityką bezpieczeństwa. Treść polityki bezpieczeństwa zawiera załącznik Nr 1 do zarządzenia.

§ 2

Wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim", zwanej dalej instrukcją. Treść instrukcji zawiera załącznik Nr 2 do zarządzenia.

§ 3

Polityka bezpieczeństwa, o której mowa w § 1 oraz instrukcja, o której mowa w § 2 mają zastosowanie na wszystkich stanowiskach pracy, na których przetwarzane są dane osobowe.

§ 4

Z treścią polityki bezpieczeństwa oraz instrukcją kierownicy referatów zapoznają pracowników zatrudnionych przy przetwarzaniu danych osobowych.

§ 5

Traci moc Zarządzenie Burmistrza Miasta i Gminy Piotrków Kujawski Nr 4/99 z dnia 28 września 1999 r.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Mirosław Słomieczny

Załącznik Nr 1
do zarządzenia Nr 52/2007
Burmistrza Miasta i Gminy Piotrków Kujawski
z dnia 6 listopada 2007 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY W PIOTRKOWIE KUJAWSKIM

§1

1. Polityka bezpieczeństwa określa:

1). Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;

2). Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3). Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4). Sposób przepływu danych miedzy poszczególnymi systemami;

5). Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności i rozliczalności przetwarzanych danych.

§2

2. Polityka bezpieczeństwa dotyczy zabezpieczenia danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim w formie tradycyjnej tj. ręcznie i w formie elektronicznej.

§3

Ilekroć w polityce bezpieczeństwa jest mowa o:

1. danych osobowych - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanych lub możliwej do zidentyfikowania osoby fizycznej;
2. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;
3. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te , które wykonuje się w systemach informatycznych;

4. wykazie zbiorów danych osobowych - rozumie się prze to wykaz zarejestrowanych oraz podlegających rejestracji zbioru danych osobowych;
5. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6. poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
7. integralności danych - rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
8. rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane tylko podmiotowi;
9. administratorze bezpieczeństwa informacji - rozumie się przez to pełnomocnika ds. ochrony informacji niejawnych;
10. administratorze systemu - rozumie się przez to osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemem informatycznym na terenie Urzędu Miasta i Gminy w Piotrkowie Kujawskim.

§4

1. Obszar, w którym przetwarzane są dane osobowe stanowią pomieszczenia budynku Urzędu Miasta i Gminy w Piotrkowie Kujawskim, ul. Kościelna 1 (parter i piętro).
2. Dane osobowe przetwarzane w sposób tradycyjny przetwarzane są w obszarach budynku, o którym mowa w ustępie 1.
3. Szczegółowy wykaz pomieszczeń, w których przetwarzane są dane osobowe prowadzi administrator bezpieczeństwa informacji z uwzględnieniem wydziałów, księgowości i oddziału administracyjnego oraz przyznanych uprawnień do korzystania z programów.
4. W zakresie, o którym mowa w ust. 4 administrator systemu współpracuje z administratorem bezpieczeństwa informacji.
5. W przypadku zmian oraz dokonywania aktualizacji obszaru, należy bezwzględnie zawiadomić o tym administratora bezpieczeństwa.

§5

1. Pracownicy przetwarzający dane osobowe zobowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy.
2. Klucze do pomieszczeń służbowych znajdują się w budynku Urzędu.
3. Kierownicy referatów (samodzielne stanowiska pracy) sprawują kontrolę nad prawidłowym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe w podległych referatach.
4. Wszelkie nieprawidłowości w zakresie, o którym mowa w ust. 3 należy niezwłocznie zgłaszać do Referatu Organizacyjnego i Spraw Obywatelskich oraz administratora bezpieczeństwa informacji.

§6

1. Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych w zbiorach, prowadzonych w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim, znajdują się w rejestrze zbioru danych, stanowiącym załącznik A do Polityki bezpieczeństwa.
2. Kierownicy referatów niezwłocznie zgłaszają administratorowi bezpieczeństwa informacji wszelkie zmiany w zbiorach danych osobowych oraz zbiory danych osobowych, które podlegają zgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych.

§7

1. Opis struktury zbiorów wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi dokonuje administrator bezpieczeństwa informacji.
2. Opis, o którym mowa w ust. 1, w odniesieniu do zbioru danych przetwarzanych w systemach informatycznych dokonuje administrator systemu.

§8

1. Środkami technicznymi i organizacyjnymi niezbędnymi dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych w systemie informatycznym Urzędu Miasta i Gminy w Piotrkowie Kujawskim są:

- system nadawania uprawnień, tj. system kont użytkowników i haseł,
- zastosowanie zapory ogniowej - firewall oraz jej bieżący monitoring,
- zastosowanie ochrony antywirusowej i antyszpiegowskiej.

2. Środki techniczne i organizacyjne, o których mowa w ustępie 1, szczegółowo określa zarządzenie „ w sprawie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim".

§9

1. Przetwarzanie danych osobowych w zbiorach prowadzonych w systemach informatycznych jest dopuszczalne wyłącznie przez osoby posiadające upoważnienia wydane przez Burmistrza Miasta i Gminy Piotrków Kujawski.
2. Osoby przetwarzające dane osobowe w sposób tradycyjny przetwarzają je na podstawie uprawnień wynikających z indywidualnych zakresów czynności.
3. Kierownicy referatów prowadzą ewidencje osób przetwarzających dane osobowe w sposób tradycyjny w zakresie działania referatu oraz dokonują zmian w zakresach czynności podległych pracowników.

§10

Kierownicy referatów zapewniają przestrzeganie polityki bezpieczeństwa w pracy referatu.

Załącznik A
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim.

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych w zbiorach, prowadzonych w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim

BURMISTRZ
mgr Mirosław Skonieczny

1) PODATKI
2) KADRY i PŁACE
3) PŁATNIK
4) GEOBAZA (Ewidencja gruntów i budynków)
5) ELUD (System Ewidencji Ludności)
6) SOO (System Obsługi Obywatela)

Załącznik Nr 2
do zarządzenia Nr 52/2007
Burmistrza Miasta i Gminy Piotrków Kujawski
z dnia 6 listopada 2007 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY W PIOTRKOWIE KUJAWSKIM

§1

Instrukcja określa:

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie odpowiedzialnych za te czynności.
2. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem.
3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.
4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania.
5. Sposób i miejsce oraz okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych określonych w pkt 4.
6. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
7. Sposób odnotowania informacji o udostępnionych danych osobowych.
8. Zasady wykonywania przeglądów konserwacji systemu oraz nośników informacji służących do przetwarzania danych.
9. Zasady użytkowania sieci komputerowej.

§2

Ilekroć w instrukcji jest mowa o:

1. Zbiorze danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.

2. Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

3. Administratorze danych osobowych - rozumie się przez to Burmistrza Miasta i Gminy Piotrków Kujawski.

4. Administratorze systemu - rozumie się przez to osoby lub osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim.

5. Identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

6. Haśle - rozumie się prze to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

7. Urzędzie - rozumie się prze to Urząd Miasta i Gminy w Piotrkowie Kujawskim.

8. Administratorze dostępu do Internetu - rozumie się przez to osobę przygotowującą i wdrażającą koncepcję podłączenia sieci lokalnej do Internetu, administrującą serwerem i innymi urządzeniami wykorzystanymi do realizacji dostępu do Internetu.

9. Administratorze bezpieczeństwa informacji - rozumie się przez to osobę lub osoby upoważnione i odpowiedzialne za przestrzeganie ustawy o ochronie danych osobowych.

10. Publicznej sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.

§3

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie wydane przez Burmistrza Miasta i Gminy Piotrków Kujawski. Upoważnienie to zawiera nazwę zbioru danych oraz zakres uprawnień użytkownika do przetwarzania danych osobowych.
2. Ewidencję upoważnień prowadzi administrator bezpieczeństwa informacji.

§4

1. Upoważnienie, o którym mowa w § 3 pkt 1, stanowi podstawę do rejestracji użytkownika systemu informatycznego.
2. Administrator systemu rejestruje osobę w systemie na wniosek administratora bezpieczeństwa informacji.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym, może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła.
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, administrator systemu ustala nieprzetwarzalny identyfikator i hasło.
5. Identyfikator użytkownika, nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. O utracie uprawnień administrator bezpieczeństwa niezwłocznie informuje administratora systemu.
7. Administrator systemu przekazując użytkownikowi identyfikator i hasło przeprowadza szkolenie użytkownika z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.
8. Administrator systemu prowadzi ewidencję użytkowników systemu informatycznego, zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Miasta

i Gminy w Piotrkowie Kujawskim. Ewidencja użytkowników powinna zawierać:

- imię i nazwisko,
- stanowisko,
- komórkę organizacyjną

§5

1. Dane osobowe przetwarzane są w sieci Urzędu Miasta i Gminy za pomocą komputerów stacjonarnych.

2. Hasło użytkownika powinno mieć najmniej 6 znaków i być zmieniane, co najmniej raz na miesiąc.

3. Hasło nie może być zapisane w miejscu dostępnym dla osób nieupoważnionych. Użytkownik nie może udostępniać identyfikatora, hasła i stanowiska roboczego osobom nieupoważnionym.

4. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego utrzymywane jest w tajemnicy również po upływie jego ważności.

5. Zapasowe hasła użytkowników systemu powinny znajdować się w zabezpieczonej kopercie w metalowej szafie.

6. Komputery, na których dane osobowe służą do edycji danych powinny być zabezpieczone hasłem składającym się z co najmniej 6 znaków i być zmieniana przynajmniej co 12 miesięcy. Pracownicy zatrudnieni przy ich obsłudze dbają o to, aby nie były one używane przez osoby nieupoważnione.

§6

1. Użytkownik wyłącza sprzęt komputerowy powiadamia administratora systemu o braku możliwości zalogowania się na swoje konto oraz o podejrzeniu fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe.

2. Po potwierdzeniu przez administratora systemu fizycznej nieuprawnionej ingerencji

w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe użytkownik:

1) niezwłocznie powiadamia o tym administratora bezpieczeństwa informacji lub upoważnioną przez niego osobę, a w przypadku ich nieobecności - bezpośrednio administratora danych osobowych,

b) sporządza notatkę służbową z opisem sytuacji wskazującej na naruszenie zabezpieczeń systemu informatycznego i przekazuje ją administratorowi bezpieczeństwa informacji,

c) administrator bezpieczeństwa informacji po zbadaniu zdarzenia z ust. 1 przygotowuje informację o przyczynach, przebiegu i wnioskach ze zdarzenia oraz przekazuje ją administratorowi danych osobowych.

§ 7

Dane osobowe są przetwarzane z użyciem systemu informatycznego w godzinach pracy Urzędu Miasta i Gminy w Piotrkowie Kujawskim. Poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody administratora bezpieczeństwa informacji, z zachowaniem warunków określonych w Regulaminie pracy Urzędu.

§ 8

1. Ekrany monitorów stanowisk, na których przetwarzane są dane osobowe powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
2. W pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień o których mowa w § 3 ust. 1 , monitory stanowisk komputerowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
3. Użytkownik ma obowiązek wylogowania się z systemu przy dłużej nieobecności na stanowisku pracy lub zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem nie może pozostać bez kontroli pracującego na nim pracownika.
4. Wydruki zawierające dane osobowe należy przechowywać w miejscu

uniemożliwiającym ich odczytanie przez osoby nieuprawnione. Wydruki nieprzydatne należy bezwzględnie zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 9

1. Przebywanie osób nieupoważnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się w obszarze, w których są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich zatrudnionych osób w sposób uniemożliwiający dostęp do nich osób trzecich.

§10

1. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu. Nośniki danych po ustaniu ich użyteczności pozbawiać danych lub niszczyć w sposób uniemożliwiający ich odczyt.
2. Kopie zapasowe miesięczne wykonywane na dyskietkach, płytach CD lub taśmach, należy przechowywać w kasie pancernej Urzędu. Kopie baz danych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w pomieszczeniach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
3. Kopie miesięczne przechowuje się przez okres 3 miesięcy. W przypadku danych księgowych okres przechowywania danych wynosi 5 lat.

§11

1. W związku z zaistnieniem zagrożenia dla zbiorów danych ze strony wirusów komputerowych oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego

dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych. Wirusy komputerowe oraz wyżej wymienione oprogramowanie mogą pojawić się w Urzędzie poprzez:

a) Internet,

b) Oprogramowanie przenoszone dyskietkami, dyskami zewnętrznymi.

2. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych:

1) Serwery, programy i zbiory danych zainstalowane na serwerze, nośniki informacji będące w bezpośrednim użytkowaniu przez administratora systemu winny być sprawdzone przez administratora systemu na obecność wirusów komputerowych co najmniej raz w tygodniu, a w razie potrzeby i częściej,

2) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego. Użytkownik komputera, w którym zainstalowany jest program antywirusowy zobowiązany jest do sprawdzenia komputera raz w tygodniu na obecność wirusów komputerowych oraz co 3 dni do dokonania aktualizacji bazy wirusów tego programu, gdy aktualizacja automatyczna nie działa,

3) Przeciwdziałanie zagrożeniom, które są związane z podłączeniem sieci lokalnej z publiczną:

- serwer i inne urządzenia wykorzystywane w realizacji dostępu do Internetu posiadają oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem do sieci lokalnej,
- administrator dostępu do Internetu monitoruje na bieżąco stan bezpieczeństwa, analizuje logi pod kątem naruszenia zabezpieczeń raz na tydzień dokonując szczegółowej analizy stanu zabezpieczeń.

§12

Użytkownik zapisuje w programie informację o odbiorcach danych osobowych (art. 7 pkt 6 ustawy o ochronie danych osobowych), którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, jeżeli system informatyczny nie jest używany do przetwarzania danych zawartych w zbiorach jawnych.

§13

1. Przeglądy i konserwacje systemu i zbiorów danych wykonuje administrator systemu na bieżąco, lecz nie rzadziej niż raz w miesiącu. Administrator sprawdza spójność danych indeksów oraz stan nośników np. dysków twardych.

2. Administrator systemu okresowo sprawdza możliwość odtwarzania danych z kopii zapisowej.

§14

Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe, należy pozbawić tych danych przed przekazaniem innemu podmiotowi. Nośniki danych zawierające dane osobowe są likwidowane poprzez uszkodzenie w sposób uniemożliwiający ich odczytanie. Naprawę wymienionych urządzeń należy wykonywać pod nadzorem osoby upoważnionej przez administratora danych lub jeśli jest to możliwe, pozbawić je danych osobowych przed wydaniem ich do naprawy.

§15

Korzystającym z systemu informatycznego w Urzędzie Miasta i Gminy w Piotrkowie Kujawskim zabrania się:

a) udostępniania stanowiska pracy oraz istniejących w nich danych osobom nieupoważnionym,

b) udostępniania osobom nieuprawnionym programów komputerowych,

c) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,

d) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,

e) samodzielnego instalowania i używania programów komputerowych; programy komputerowe instalowane są przez administratora systemu lub za jego zgodą przez inną upoważniona osobę,

f) używania nośników danych udostępnionych przez osoby nieuprawnione,

g) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z pracą.

W przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy te nośniki przeskanować programem antywirusowym, jeżeli program antywirusowy nie jest zainstalowany na danej stacji roboczej należy to zrobić na innym stanowisku.

g) wykorzystania sieci komputerowej w celach innych, niż wyznaczone przez administratora danych osobowych.

BURMISTRZ

mgr Mirosław Skonieczny