Zarządzenie Nr 59/07
Burmistrza Łap
z dnia 28 września 2007r.

w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych

Na podstawie art. 31 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2001r. Nr 142, poz. 1592 z późn. zm.) i art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) w związku z § 3 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) zarządzam, co następuje:

§ 1.

1. Wprowadzam dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w systemie wydawania dowodów osobistych w Urzędzie Miejskim w Łapach.
2. Na dokumentację, o której mowa w ust. 1 składa się:
   1) Instrukcja zarządzania systemem informatycznym służącym do ewidencji wydawanych dowodów osobistych w Urzędzie Miejskim w Łapach stanowiąca załącznik nr 1 do zarządzenia,
   2) Polityka bezpieczeństwa informacji systemu wydawania dowodów osobistych w Urzędzie Miejskim w Łapach stanowiąca załącznik nr 2 do zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do Zarządzenia nr 59/07
Burmistrza Łap
z dnia 28 września 2007r

INSTRUKCJA ZARZĄDZANIA
systemem informatycznym służącym do ewidencji wydawanych dowodów osobistych w Urzędzie Miejskim w Łapach

§1.

Administratorem danych, w tym także danych w systemie informatycznym służącym ewidencji wydawanych dowodów osobistych w Urzędzie Miejskim w Łapach jest Burmistrz Łap.

§2.

1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przed osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. W celu zrealizowania tych obowiązków administrator danych wprowadza instrukcję zarządzania systemem informatycznym służącym do ewidencji wydawanych dowodów osobistych jako dokument obowiązujący w Urzędzie Miejskim w Łapach.

§3.

Administrator danych zobowiązuje podwładnych do przestrzegania postanowień tej instrukcji.

§4.

1. Przez administratora bezpieczeństwa informacji należy rozumieć osobę lub osoby upoważnione przez Administratora danych osobowych do administrowania i zarządzania systemami informatycznymi na terenie obszaru.

2. W Urzędzie Miejskim w Łapach administratorem bezpieczeństwa informacji jest osoba pracująca na stanowisku ds. informatyki. Z administratorem bezpieczeństwa informacji można kontaktować się pod nr telefonu 085 715 22 51 wew. 148

§5.

1. Przetwarzanie danych osobowych to wykonywanie na nich operacji takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie zarówno w systemie informatycznym jak i ręcznym.

2. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, o którym mowa w pkt. 3 osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

3. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności w nich osób zatrudnionych w sposób uniemożliwiający dostęp do nich osób trzecich.

§6.

Procedura rozpoczęcia i zakończenia pracy:

- na stanowiskach, na których przetwarzane są dane osobowe ekrany monitorów powinny być tak ustawione, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych,
- bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po włożeniu karty, podaniu identyfikatora i właściwego hasła,
- każdy z użytkowników korzystając z systemów przetwarzających dane osobowe powinien posiadać swoją kartę, identyfikator i hasło,
- hasła powinny być zmieniane raz w miesiącu i składać się z co najmniej 6 znaków (najlepiej z liter i cyfr),
- hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępniać karty, identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym,
- użytkownik powinien upewnić się, że osoby nie upoważnione nie mają możliwości wglądu do danych,
- w razie przerwania pracy konieczne jest zastosowanie wygaszacza ekranu,
- użytkownik powinien upewnić się czy dane zostały zarejestrowane, aby uniknąć utraty danych z powodu awarii,
- podczas nieobecności osób zatrudnionych przy informatycznym przetwarzaniu danych osobowych pomieszczenia, w których przetwarzane są dane, nie mogą być udostępniane osobom postronnym,
- zakończenie pracy związanej z przetwarzaniem danych powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.

§7.

Rejestr użytkowników systemów informatycznych prowadzi Administrator bezpieczeństwa. W rejestrze użytkowników znajdują się następujące dane:

- nazwisko i imię,
- identyfikator,
- stanowisko,
- referat, w którym użytkownik jest zatrudniony,

- wskazanie zbiorów, do których użytkownik jest uprawniony,
- zakres uprawnień do systemów.

W przypadku wyrejestrowania użytkownika jego identyfikator nie może być przekazany innemu pracownikowi.

3. Zabrania się użytkownikom systemu informatycznego:

- udostępniania stanowisk roboczych oraz istniejących w nich danych (w postaci pisemnej lub elektronicznej) osobom nieupoważnionym,
- wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez administratora danych osobowych,
- samowolnego instalowania i użytkowania programów komputerowych (posiadających lub nie posiadających licencji),
- trwałego lub okresowego kopiowania programów w całości lub części bez zgody administratora systemu,
- publicznego rozpowszechniania programów komputerowych lub ich kopii dla osób postronnych,
- przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
- udostępniania osobom postronnym programów komputerowych
- używania nośników udostępnianych przez osoby postronne i podejrzanych o „zainfekowanie wirusem" ; w razie podejrzenia o „zainfekowanie wirusem" nośnika danych (dyskietki lub dysku twardego) użytkownik ma obowiązek niezwłocznie poinformować o tym administratora danych osobowych lub inna uprawnioną osobę,
- używania oprogramowania w większym zakresie niż pozwala na to umowa licencyjna,

4. Czas pracy przy urządzeniach informatycznych jest tożsamy z godzinami pracy Urzędu, wynikającymi z Regulaminu Urzędu Miejskiego w Łapach

5. Na pracę przy urządzeniach informatycznych poza godzinami pracy konieczna jest zgoda administratora systemu.

Załącznik nr 2
do Zarządzenia nr 59/07
Burmistrza Łap z dnia 28
września 2007r.

Polityka bezpieczeństwa informacji systemu do wydawania dowodów osobistych w Urzędzie Miejskim w Łapach

1. Pojęcie danych osobowych
   a) Zgodnie z art.6 ust.1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 1, poz. 926 ze zmianami) za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
   b) Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, albo jeden lub kilka specyficznych określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2 ustawy).
   c) Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Daną osobową będzie taka informacja, która pozwala na ustalenie tożsamości danej osoby, bez nadzwyczajnego wysiłku i nakładu zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł.

2. Ochrona danych osobowych

Ochrona polega na organizacyjnym i technicznym zabezpieczeniu danych osobowych, w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji co jednocześnie naruszałoby ochronę prywatności, prawa i wolności obywateli.

3. Pojęcie polityki bezpieczeństwa

Pojęcie „polityka bezpieczeństwa" należy rozumieć jako, zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Urzędu Miejskiego.

Zgodnie z art. 36 ust. 2 oraz art. 39a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926 ze zmianami), zwanej dalej ustawą, polityka bezpieczeństwa, powinna się odnosić całościowo do problemu zabezpieczenia danych osobowych zarówno do danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych.

4. Cel polityki bezpieczeństwa.

Celem polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

5. Bezpieczeństwo danych.

Kierownictwo Urzędu uznaje jako jeden z priorytetów zabezpieczania danych osobowych, zapewniając środki techniczne i organizacyjne jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

6. Obowiązki administratora systemu.

Upoważnieni pracownicy do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się i przestrzegania niniejszej polityki bezpieczeństwa wraz z instrukcją zarządzania systemem informatycznym (załącznik nr 2) oraz bieżącego śledzenia aktów normatywnych dotyczących ochrony danych osobowych.

7. Środki techniczno-organizacyjne.

a) Ochronę fizyczną obiektu (obszaru) stanowią drzwi antywłamaniowe oraz system alarmowy połączony bezpośrednio z firmą monitorującą.
b) Przebywanie na terenie Urzędu.
   Pracownikom wolno przebywać na terenie Urzędu tylko w godzinach ich pracy, a w przypadku konieczności pozostania po godzinach pracy w siedzibie Urzędu, fakt ten należy zgłosić Kierownikowi Urzędu lub Sekretarzowi Gminy oraz wpisać się do książki wejść i wyjść Urzędu Miasta. Osoba przebywająca na terenie Urzędu w dni wolne od pracy obowiązana jest każdorazowo:
   - dokonać zarejestrowania przyjścia zgodnie z godziną przyjścia,
   - dokonać zarejestrowania wyjścia, zgodnie z godziną wyjścia – w wyłożonej liście obecności.
c) Zabezpieczenie pomieszczeń służbowych.
   Pomieszczenia służbowe winny być zamknięte każdorazowo pod nieobecność osób w nich pracujących. Pracownicy mają obowiązek zdania kluczy od biur po zakończeniu pracy do Referatu Administracyjno-Gospodarczego. Pozostawienie kluczy w zamkach jest niedopuszczalne.

8. Wykaz pomieszczeń i zbiorów tworzących obszar, w którym przetwarzane są dane osobowe.

   Zbiory danych osobowych znajdujących się w chronionym obszarze gromadzone i przetwarzane są w pomieszczeniu: ewidencja wydawanych dowodów osobistych – pokój nr 112.