Załącznik nr 2 do zarządzenia nr 316)06
BMiG Małogoszcz z dnia 31 lipca 2006r.

INSTRUKCJA
PRZETWARZANIA DANYCH OSOBOWYCH
W URZĘDZIE MIASTA I GMINY MAŁOGOSZCZ

Rozdział I
Zasady ogólne

§ 1

Instrukcja została opracowana na podstawie ustawy z dnia 29 sierpnia 1997 roku
ochronie danych osobowych *(Dz. U z 2002 r.Nr 101, poz.926 z późn.zm.)* w celu realizacji 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 z 2004 r. .nr 100, poz. 1024)*.

§ 2

Przez użyte w Instrukcji następujące określenia należy rozumieć:

1) **dane osobowe** — każda informacja dotycząca osoby fizycznej, pozwalającej na określenie tożsamości tej osoby,
2) **zbiór danych osobowych** — każdy posiadający strukturę zestaw danych o charakterze osobowym dostępny według określonych kryteriów,
3) **przetwarzanie danych** —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) **Administrator Danych Osobowych** — Burmistrz
5) **Administrator Bezpieczeństwa Informacji** — osoba wyznaczona przez administratora danych osobowych odpowiedzialna za bezpieczeństwo danych osobowych,
6) **Urząd** — Urząd Miasta i Gminy Małogoszcz,
7) **Skarbnik gminy. Kierownik referatu Budownictwa i Inwestycji -kierownik referatu** ,
8) **pracownik samorządowy** — osoba zatrudniona w ramach stosunku pracy w Urzędzie,

9) **użytkownik** - osoba przetwarzająca dane,
10) **system informatyczny** — zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych,
11) **zwrotna informacja telefoniczna** — czynności polegające na:
- przyjęciu wniosku telefonicznego o udostępnienia danych wraz z informacją o tożsamości, nazwie jednostki organizacyjnej oraz numerze wnioskodawcy,
- oddzwonieniu ze stosowną informacją bądź danymi, po uprzednim sprawdzeniu prawdziwości i autentyczności wnioskodawcy.

§ 3.

Do kompetencji Administratora Danych Osobowych należy prowadzenie całokształtu spraw związanych z przetwarzaniem danych osobowych, a w szczególności:
1) udostępnianie danych osobowych,
2) kontrola i nadzór w zakresie przestrzegania zasad i procedur przetwarzania danych osobowych w Urzędzie, z uwzględnieniem kryterium celowości i adekwatności oraz warunków organizacyjno-technicznych,
3) rejestracji zbiorów danych osobowych w rejestrze Generalnego Inspektora Ochrony Danych Osobowych,
4) prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych,
5) podpisywanie umowy o powierzenie danych osobowych podmiotowi zewnętrznemu oraz kontrolę przestrzegania prawa przez strony umowy,
6) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 4

Administrator bezpieczeństwa informacji, z upoważnienia administratora danych osobowych:
1) zarządza i nadzoruje systemem informatycznym, gdzie przetwarzane są dane osobowe,
2) podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
3) czuwa nad wdrażaniem niniejszej Instrukcji w systemach informatycznych, w których przetwarzane są dane osobowe oraz dba o bieżące jej uaktualnienie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,
4) współpracuje z administratorem danych osobowych w zakresie aktualizacji wykazu pracowników, którzy posiadają upoważnienia do przetwarzania

danych osobowych,
5) prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów,
6) prowadzi ewidencję miejsc przetwarzania danych osobowych i sposobu zabezpieczenia,
7) pełni rolę Administratora Systemów Informatycznych.
8) Administrator Bezpieczeństwa Informacji zobowiązany jest do współpracy
z Administratorem Danych Osobowych w zakresie aktualizacji wykazu pracowników, którzy posiadają upoważnienia do przetwarzania danych osobowych.

§ 5

1. Kierownik referatu wykonuje czynności przetwarzania danych osobowych w ramach zbiorów, funkcjonujących w podległym referacie z upoważnienia administratora danych osobowych.
2. Kierownik referatu sprawuje bezpośredni nadzór nad przetwarzaniem danych osobowych w referacie i jest zobowiązany do kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych osobowych przez podległych pracowników. Wzór upoważnienia stanowi załącznik nr 1 do instrukcji.
3. Pracownik referatu, pracownik na samodzielnym stanowisku dokonuje czynności przetwarzania danych osobowych, z upoważnienia Administratora Danych Osobowych, w zakresie indywidualnych obowiązków pracowniczych. Wzór upoważnienia stanowi załącznik nr 2 do instrukcji.
4. Administrator Danych Osobowych prowadzi wykaz potwierdzeń odbioru upoważnień dostępu do danych osobowych według wzoru określonego w załączniku nr 3 do instrukcji.

Rozdział III
Obowiązki pracowników

§ 6

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.

§ 7

1. Osoby, wymienione wszystkich § 4 są zobowiązane do:

   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   2) stosowania określonych przez Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne przetwarzanie danych,
   3) należytego zabezpieczenia danych przed ich udostępnieniem osobom nie upoważnionym,
   4) zachowanie szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą,
   5) sygnalizowania niezgodności aktów prawnych gminy oraz innych aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej,
   6) zwracanie się do Administratora Danych Osobowych, w przypadku wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych o wiążące wytyczne.

§ 8

Pracownik, któremu Administrator Danych Osobowych udzielił upoważnienia do przetwarzania danych osobowych jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik nr 4 do instrukcji.

Rozdział IV
Procedury szczegółowe

§ 9

1. W przypadku przyjęcia do pracy nowego pracownika referatu, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, kierownik referatu zobowiązany jest zwrócić się do Administratora Danych Osobowych o wydanie upoważnienia do przetwarzania danych osobowych,

zaś w przypadku przyjęcia do pracy na samodzielne stanowisko nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, upoważnienia do przetwarzania danych osobowych wydaje bezpośrednio Administrator Danych Osobowych.

2. Pracownik, któremu udzielono stosowne upoważnienie, o którym mowa w ust. 1 jest zobowiązany do podpisania oświadczenia, którego wzór stanowi załącznik nr 4 do niniejszej instrukcji.
3. W przypadku zmiany stanowiska, zakresu obowiązków pracowniczych, kierownik referatu zobowiązany jest bezzwłocznie skierować wniosek o wydanie bądź cofnięcie stosownego upoważnienia do Administratora Danych Osobowych.
4. W przypadku zamiany samodzielnego stanowiska, zakresu obowiązków pracowniczych na tym stanowisku wydanie bądź cofnięcie upoważnienia dokonuje bezpośrednio Administrator Danych Osobowych.
5. Wzór do zmiany zakresu obowiązków pracownika przetwarzającego dane osobowe stanowi załącznik nr 5 do instrukcji.
6. Wzór do pozbawienia pracownika upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 6 instrukcji.
7. Administrator Danych Osobowych prowadzi wykaz pracowników pozbawionych upoważnień do przetwarzania danych osobowych według wzoru określonego w załączniku nr 7 do instrukcji.

§ 10

1. W przypadku nawiązania stosunku pracy na stanowisku zastępcy burmistrza, sekretarza gminy których zakres obowiązków obejmować będzie przetwarzanie danych osobowych, upoważnienie do przetwarzania wydaje bezpośrednio Administrator Danych Osobowych według załącznika nr 1.
2. W przypadku zmiany na stanowisku zastępcy burmistrza, sekretarza gminy, kierownika referatu wydanie bądź cofnięcie upoważnienia dokonuje bezpośrednio Administrator Danych Osobowych.

§ 11

1. Rozwiązanie stosunku pracy w okresie obowiązywania upoważnienia powoduje jego wygaśnięcie, z zastrzeżeniem ust.2.
2. Wypowiedzenie umowy o pracę przez pracodawcę powoduje wygaśnięcie upoważnienia do przetwarzania danych z dniem wręczenia wypowiedzenia umowy o pracę.

§12

W przypadku konieczności utworzenia nowego zbioru danych, wynikającej z obowiązków nałożonych przepisami ustawy bądź nowymi zadaniami,

kierownik referatu, pracownik na samodzielnym stanowisku pracy zobowiązany jest niezwłocznie — nie później niż w ciągu 30 dni od dnia powstania obowiązku utworzenia zbioru — złożyć Administratorowi Danych Osobowych, projekt wniosku o zarejestrowanie zbioru danych osobowych, którego wzór stanowi załącznik nr 8 do niniejszej instrukcji.

§ 13

1. W obiegu zewnętrznym dane osobowe udostępnia ze zbiorów zgodnie z powszechnie obowiązującymi w tym zakresie przepisami, Administrator Danych Osobowych lub osoba przez niego upoważniona.
2. W obiegu wewnętrznym między pracownikami Urzędu, chyba że przepisy szczególne stanowią inaczej można udostępniać dane osobowe w następującym trybie: informacje zawierające dane: imię i nazwisko, adres zamieszkania i inne o charakterze podstawowym bezpośrednio identyfikujące osobę fizyczną może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej".
3. Tryb określony w ust.2, może być w uzasadnionych przypadkach stosowany również w wymianie informacji i danych osobowych między pracownikami Urzędu a jednostkami organizacyjnymi gminy.
4. Przekazywanie danych w trybie ust.2 i 3, może odbywać się tylko i wyłącznie w przypadku toczącego się postępowania administracyjnego bądź cywilnego w stosunku do osoby, której dane dotyczą.
5. Udostępnianie danych osobowych, o których mowa w ust. 1 jest udokumentowane w „rejestrze" prowadzonym przez pracowników Urzędu, którzy przetwarzają właściwe zbiory.

§ 14

1. W umowach zawieranych przez Burmistrza w przypadku zaistnienia okoliczności powierzenia danych osobowych podmiotowi zewnętrznemu w celu wykonania określonych czynności na tych danych, każdorazowo wymagany jest zapis o powierzeniu danych osobowych bądź zawarciu odrębnej umowy powierzenia.
2. W przypadkach, o których mowa w ust. 1 kierownik referatu, bądź pracownik na samodzielnym stanowisku pracy, nie później niż w ciągu 15 dni:
   1) przed podpisaniem umowy, w której został zawarty zapis o powierzeniu,
   2) przed datą planowanego powierzenia danych, na podstawie odrębnej umowy powierzenia przekazuje Administratorowi Danych Osobowych projekt umowy, o której mowa w pkt. 1 lub projekt umowy, o której mowa w pkt.2.

Rozdział IV
Zarządzanie systemem informatycznym służącym przetwarzaniu danych osobowych.

§ 15

Uwzględniając kategorie danych osobowych oraz stopień bezpieczeństwa ich przetwarzania w systemie informatycznym Urzędu wprowadza się poziom bezpieczeństwa - **wysoki**.

§ 16

Do obowiązków Administratora Bezpieczeństwa Informacji należy wdrażanie i kontrola stosowania środków technicznych, służących do zabezpieczenia systemu informatycznego Urzędu w celu realizacji wymogów rozliczalności, poufności i integralności, w szczególności:

1) nadawanie uprawnień użytkownikowi,
2) stosowanie mechanizmów uwierzytelnienia użytkownika,
3) kontrola dostępu do danych osobowych i zbiorów danych osobowych,
4) stosowanie środków ochrony w ramach oprogramowania urządzeń teletransmisyjnych, systemów, narzędzi i systemu użytkowego,
5) administrowanie sprzętem informatycznym,
6) zapewnienie właściwej obsługi sprzętowej i programowej przez stanowiska pracy w celu zapewnienia właściwego standardu jakości przetwarzania.

§ 17

Kierownik referatu, pracownik na samodzielnym stanowisku pracy zobowiązany jest do:

1) każdorazowego informowania Administratora Bezpieczeństwa Informacji o planowanych przemieszczeniach sprzętu komputerowego między pokojami, gdzie dokonuje się czynności przetwarzania danych,
2) zapewnienia odpowiednich warunków organizacyjno-technicznych umożliwiającym zachowanie poufności informacji (dostęp do pomieszczeń szaf z aktami),
3) nadzorowania warunków przechowywania wydruków zawierających dane osobowe, ich archiwizowanie i okresowe niszczenie oraz przechowywanie danych osobowych na dyskietkach i CD/DVD-ROM-ach,

4) wnioskowania o przyznanie sprzętu komputerowego niezbędnego do wykonywania wyznaczonych czynności w systemie informatycznym i przyznanie identyfikatora.

§ 18

Szczegółowe wdrożenie programowych i sprzętowych rozwiązań w zakresie zabezpieczenia danych osobowych w referacie i na samodzielnych stanowiskach
zapewnia Administrator Bezpieczeństwa Informacji.

§ 19

1. Dla każdego stanowiska pracy przetwarzającego dane osobowe Administrator Bezpieczeństwa Informacji nadaje uprawnienia dostępu do danych osobowych w formie identyfikatora i hasła.
2. Identyfikator osoby, która utraciła uprawnienie dostępu do danych osobowych Administrator Bezpieczeństwa Informacji jest zobowiązany unieważnić jej hasło oraz podjąć inne stosowne działanie w celu zapobieżenia
dalszemu dostępowi tej osoby do danych.
3. Realizując obowiązki, o których mowa w ust. 1 i 2 prowadzi się ewidencję identyfikatorów.

§ 20

1. Każdy pracownik przetwarzający dane osobowe zobowiązany jest do posługiwania się przydzielonym hasłem, zmienianym co miesiąc oraz identyfikatorem, który nie powinien być zmieniany.
2. Zmiana hasła następuje raz w miesiącu, następnych zmian hasła dokonuje pracownik pod kontrolą Administratora Bezpieczeństwa Informacji.
3. Hasło, o którym mowa w ust.2 składa się z co najmniej 8 znaków.w tym dużych i małych liter oraz cyfr.

§ 21

Pracownik przetwarzający dane osobowe zobowiązany jest:
1. przystępując do pracy podać dane dostępu do komputera, zaś kończąc pracę prawidłowo zakończyć jego użytkowanie,
2. posługiwać się jedynie programami autoryzowanymi,
3. wykonywać wydruki związane z przetwarzaniem
danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów zawodowych,

4. przechowywać wydruki z danymi osobowymi w zamykanych i zabezpieczonych sejfach lub szafach,
5. w przypadku przetwarzania zbiorów danych osobowych poza bazą informatyczną pracownik jest zobowiązany przetwarzać zbiór na dysk K,
6. tworzyć kopie zapasowe baz informatycznych w ilości 1 szt,
7. tworzyć kopie zapasowe plików przetwarzanych na dysku K w ilości 1 szt,
8. przeprowadzać kontrolę antywirusową,
9. archiwizować pliki na dzień 31 grudnia każdego roku.

§ 22

1. Kopie zapasowe, o których mowa w 21 pkt. 6 i 7 są przechowywane przez okres 14 dni.
2. Archiwum plików, o których mowa w 21 pkt. 9 jest przechowywany przez okres 5 lat na odrębnych nośnikach informatycznych w wydzielonych i zabezpieczonych pomieszczeniach poza obszarem przetwarzania.
3. Po upływie okresu, o którym mowa w ust. 2 Administrator Bezpieczeństwa Informacji na wniosek pracownika może przedłużyć okres przechowywania archiwum plików ze względu na ich znaczenie prawne, organizacyjne bądź techniczne dokumentów bądź zapisów tam zawartych.
4. W przypadku korzystania z nośników elektronicznych, pochodzących od podmiotu zewnętrznego, pracownik zobowiązany jest do sprawdzania go programem antywirusowym.
5. Nośniki elektroniczne są przechowywane przez czas ich użyteczności poza obszarem przetwarzania danych osobowych a następnie dane z nich są usuwane bądź nośniki fizycznie niszczone są za zgodą Burmistrza.
6. Administrator Danych Osobowych prowadzi ewidencję sposobów, miejsc i okresów przechowywania kopii zapasowych.

§ 23

1. Komputery przenośne na pisemny wniosek Burmistrza zostają przekazane do użytkowania wskazanym pracownikom po podpisaniu protokołu odbioru.
2. Komputery przenośne posiadają zabezpieczenie techniczne, celem których jest poufność danych osobowych, jednakże zakazane jest tworzenie i przetwarzanie danych osobowych.

§ 24

1. Naprawa sprzętu informatycznego odbywa się na wniosek pracownika przetwarzającego zbiory danych osobowych pod nadzorem Administratora Bezpieczeństwa Informacji, który:
   1) sprawdza zawartość zbiorów, podejmuje decyzje o sposobie ochrony

zbiorów danych poprzez alternatywny wybór:
a) bezpośredniego nadzoru w czasie naprawy
b) pozbawienie zapisu, uniemożliwiających ich odzyskanie
2) wprowadza instrumenty ochrony, o których mowa w pkt.1 lit.a i b, nadzoruje sposób i zakres naprawy sprzętu.

2. Pracownik potwierdza pisemnie odbiór sprzętu po naprawie i sprawdza zapisy, w nim zawarte.
3. Likwidacja bądź przekazanie sprzętu komputerowego, na którym przetwarza się dane osobowe następuje po całkowitym pozbawieniu zapisu danych bądź uszkodzenie w sposób uniemożliwiający ich odczytanie.
4. Administrator Bezpieczeństwa Informacji prowadzi ewidencję prac serwisowych i konserwacyjnych sprzętu informatycznego według wzoru określonego w załączniku nr 9 do instrukcji.

§ 25

1. W pomieszczeniach, w których dokonuje się czynności przetwarzania danych, osoby nieuprawnione do dostępu do danych osobowych mogą przebywać wyłącznie w obecności osoby zatrudnionej przy przetwarzaniu danych.
2. Pomieszczenia, o których mowa w ust. l, na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, muszą być zamykane w sposób uniemożliwiający dostęp do nich osób postronnych.

§ 26

Urządzenia służące przetwarzaniu danych zasilane energią elektryczną muszą być przez cały czas zabezpieczone przed utratą tych danych spowodowanych awarią zasilania lub zakłóceniami sieci zasilającej.

§ 27

Ekrany monitorów na stanowiskach z dostępem do danych osobowych winny być automatycznie wyłączane po upływie nie dłużej niż 3 minut nieaktywności pracownika za pomocą systemowych wygaszaczy zabezpieczonych hasłem.

§ 28

1. Dla każdej osoby, której dane są przetwarzane powinno być odnotowane:
   a) data pierwszego wprowadzenia danych tej osoby,
   b) dane odbiorców, którym dane zostały udostępnione, jeśli przewidziane jest ich udostępnianie innym podmiotom, chyba, że dane te traktuje się jako dane jawne.
2. W uzasadnionych przypadkach uniemożliwiających odnotowywanie,

o którym mowa w ust. 1 pracownicy prowadzą wydzielony rejestr odbiorców, którym udostępniono dane osobowe ze zbiorów.

Rozdział V

Postępowanie w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego

§ 29

Pracownik przetwarzający dane osobowe zobowiązany jest zawiadomić Administratora Bezpieczeństwa Informacji o każdym naruszeniu zabezpieczenia dostępu do użytkowania komputera polegającym na:

1. naruszeniu hasła dostępu,
2. częściowym lub całkowitym braku bazy danych,
3. braku możliwości uruchomienia właściwej aplikacji (programu komputerowego),
4. zmianie położenia sprzętu komputerowego.

§ 30

1. Administrator Bezpieczeństwa Informacji, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:
   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   b) podjąć działania zabezpieczające system przed ponownym naruszeniem,
   c) sporządzić protokół dokonanych czynności.
2. Protokół, o którym mowa w ust. 1 lit.c przekazuje się niezwłocznie, jednakże nie później niż w ciągu 3 dni Administratorowi Danych Osobowych.
3. Administrator Bezpieczeństwa Informacji prowadzi raport o stwierdzeniu naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub innym zbiorze według wzoru określonego w załączniku nr 10 do protokołu.

§ 31

1. W przypadku kradzieży sprzętu informatycznego z pomieszczeń pracownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji.

2. W sytuacji o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji powiadamia Administratora Danych Osobowych.

§ 32

W sytuacji, o której mowa w **§**31 decyzję o dalszym trybie postępowania w zakresie powiadomienia właściwych organów oraz podjęcia innych, szczególnych czynności zabezpieczających wskazania podejmuje Administrator Danych Osobowych.

§ 33

Administrator Bezpieczeństwa Informacji składa raz na rok Administratorowi Danych Osobowych kompleksową analizę zabezpieczeń dostępu do urządzeń służących przetwarzaniu danych osobowych ,oraz założenia strategii i polityki zabezpieczenia systemów informatycznych.

Burmistrz

Jan Głogowski