Wójt Gminy
Buczkowice

ZARZĄDZENIE Nr 10
Kierownika Urzędu Gminy Buczkowice
z dnia 30 czerwca 2003r.

w sprawie wprowadzenia instrukcji dotyczącej ochrony danych osobowych.

Działając na podstawie art.36 ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz.926)
§ 6 i §11 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz.521 ze zmianami)

zarządzam co następuje;

§ 1

1.W celu uregulowania spraw związanych z ochroną danych osobowych zgodnie z wymaganiami wynikającymi z obowiązujących w tym zakresie przepisów wprowadzam:

1) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, stanowiącą załącznik nr 1 do zarządzenia,
2) instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do zarządzenia.

2. Instrukcje, o których mowa w § 1 pkt 1 obowiązują wszystkich pracowników zatrudnionych w Urzędzie Gminy Buczkowice przy przetwarzaniu tych danych.

3.Postanowienia instrukcji, w których jest mowa o „ pracownikach" stosuje się odpowiednio także do innych osób urzędowo upoważnionych do takiego dostępu do zbioru danych osobowych, który umożliwia dokładniejsze zapoznanie się z tymi danymi, w szczególnści do osób wdrażających system przetwarzania danych osobowych, osób odbywających w urzędzie aplikację lub praktykę zawodową albo szkolenie, studentów zbierających materiały do prac dyplomowych itp.

§ 2

1.Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych pracownik powinien być zaznajomiony z przepisami dotyczącymi ochrony danych osobowych. Odbycie przeszkolenia pracownik potwierdza pisemnym oświadczeniem, które włącza się do akt osobowych pracownika.Wzór oświadczenia stanowi załącznik nr 3 do zarządzenia.

2.Indywidualne zakresy czynności pracowników zatrudnionych przy przetwarzaniu danych osobowych powinny określać stopień ich odpowiedzialności za ochronę tych danych przed niepowołanym dostępem,nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem- odpowiednio do zadań danego pracownika przy przetwarzaniu danych osobowych.

§ 3

1. Administrator danych określa pomieszczenia lub części pomieszczeń tworzące obszar , w którym są przetwarzane dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

2. Przebywanie wewnątrz obszaru, o którym mowa w ust.1, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

3. Pomieszczenia w których są przetwarzane dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osobom trzecim.

§ 4

1.Wykonanie zarządzenia oraz bieżącą kontrolę przestrzegania jego postanowień powierzam administratorowi bezpieczeństwa informacji, a w zakresie wynikającym z § 2 niniejszego zarządzenia także bezpośrednim przełożonym pracowników zatrudnionych w urzędzie przy przetwarzaniu danych osobowych.

2. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Józef Caputa

Załącznik nr 1
do Zarządzenia Nr 10
Kierownika Urzędu Gminy Buczkowice
z dnia 30 czerwca 2003r.

I N S T R U K C J A
postępowania w sytuacji naruszenia ochrony danych osobowych

I. Postanowienia ogólne

§1. Instrukcja określa sposób postępowania pracowników zatrudnionych przy przetwarzaniu w przypadku naruszenia ochrony danych osobowych, w szczególności w razie gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego, w którym przetwarza się dane osobowe, lub
2) na naruszenie zabezpieczeń tych mogą wskazywać:
   a) stan urządzeń do przetwarzania danych osobowych,
   b) zawartość zbioru danych osobowych,
   c) ujawnione metody pracy,
   d) sposób działania programu,
   e) jakość komunikacji w sieci telekomunikacyjnej.

§ 2. W razie stwierdzenia, że zaistniała którakolwiek z wyżej wymienionych sytuacji **pracownik, który to stwierdził**, jest zobowiązany do:

1) zgłoszenia tego faktu swojemu bezpośredniemu przełożonemu lub administratorowi bezpieczeństwa informacji,
2) zastosowania środków uniemożliwiających dalszą przacę systemu, jak w szczególności;
   a) zablokowanie komputera,
   b) odcięcie dostępu do systemu jego użytkownikom oraz osobom postronnym;
3) zastosowania niezbędnych środków mających na celu ochronę danych osobowych i przeciwdziałanie pogłębianiu się szkód;
4) zabezpieczenia dowodów mogących posłużyć do wyjaśnienia przyczyn i okoliczności naruszenia danych osobowych.

§ 3. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszeniu ochrony danych osobowych jest obowiązany:

1) niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji, a jeżeli nie jest to możliwe-kierownika urzędu, chyba że wcześniej zrobił to pracownik, który stwierdził naruszenie,

2) do czasu wydania odmiennych decyzji przez administratora bezpieczeństwa danych- przejąć nadzór nad pracą systemu, odsuwając od niej pracownika dotychczas zatrudnionego na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych, chyba że nie jest to możliwe lub nie ulega wątpliwości, iż naruszenie nie zostało przez pracownika popełnione umyślnie.

§ 4. Administrator bezpieczeństwa informacji powiadamia o naruszeniu ochrony danych osobowych;

1) kierownika urzędu-chyba że został on już o tym powiadomiony w trybie § 2 pkt 1 lub § 3 pkt 1 instrukcji,
2) osobę odpowiedzialną za kontrolę wewnętrzną urzędu.

§ 5. Administrator bezpieczeństwa informacji lub upoważniona przez niego osoba podejmuje czynności wyjaśniajace, majace na celu ustalenie:

1) przyczyn i okoliczności naruszenia,
2) skutków naruszenia,
3) osoby lub osób winnych naruszenia.

§ 6. Po dokonaniu ustaleń, o których mowa w § 4, **administrator bezpieczeństwa informacji** przedstawia kierownikowi urzędu:

1) ustalenia w sprawie przyczyn i okoliczności naruszenia ochrony danych osobowych,
2) propozycje działań zmierzających do przywrócenia stanu sprzed naruszenia ochrony danych osobowych,
3) propozycje dotyczące zastosowania w przyszłości środków zapobiegawczych,

4) skonsultowaną z radcą prawnym, opinię co do ewentualnego powiadomienianorganów ścigania o popełnieniu przestępstwa przeciwko ochronie danych osobowych (art. 49 i następne ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych – Dz.U. Nr 133, poz. 883) lub przeciwko ochronie informacji (rozdział XXXIII kodeksu karnego).

WÓJT
Józef Caputa

Załącznik nr 2
do Zarządzenia Nr 10
Kierownika Urzędu Gminy Buczkowice
z dnia 30 czerwca 2003r.

INSTRUKCJA
w sprawie sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

W celu zapewnienia bezpieczeństwa informacji wprowadza się następujące szczegółowe zasady zarządzania systemami informatycznymi Urzędu Gminy w Buczkowicach służącymi do przetwarzania danych osobowych.
Wszystkie systemy informatyczne działające w Urzędzie Gminy w Buczkowicach zawierające dane osobowe podlegają ochronie na mocy ustawy z dnia 29 sierpnia 1997r.o ochronie danych osobowych (Dz. U: Nr 133 poz.883) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80 poz. 521).

I. Postanowienia ogólne

§1. Niniejsza instrukcja reguluje sposób zarządzania systemami informatycznymi Urzędu Gminy w Buczkowicach, a w szczególności określa:
1) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany,
2) określenie sposobu rejestrowania i wyrejestrowywania użytkowników,
3) procedury rozpoczęcia i zakończenia pracy,
4) metodę i częstotliwość tworzenia kopii awaryjnych,
5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
6) sposób postępowania ze sprzętem komputerowym i nośnikami danych,
7) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych.

§2. Użyte w instrukcji wyrażenia oznaczają:
1) dane osobowe- każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby;

2) kopie zapasowe- kopie awaryjne oraz kopie bezpieczeństwa;

3) przetwarzanie danych osobowych- wszelkie 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) system informatyczny- system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi , który dostarcza i rozprowadza informację;

5) usuwanie danych osobowych- zniszczenie danych osobowych lub ich anonimizację, czyli taką modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

6) zabezpieczenie systemu informatycznego- środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją , zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

7) zbiór danych osobowych- każdy posiadający strukturę , zestaw danych o charakterze osobowym , dostępnych według określonych kryteriów, niezależnie od tego , czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, jak również niezależnie od stosowanej techniki przetwarzania danych. Zbiorami takimi są w szczególności systemy informatyczne, kartoteki skorowidze, księgi, wykazy i inne zbiory ewidencyjne.

II. Identyfikatory i hasła użytkowników systemów informatycznych Rejestowanie i wyrejestrowywanie użytkowników

§1. System informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizm uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych.

§2. Dla każdego użytkownika systemu informatycznego , w którym przetwarza się dane osobowe, administrator danych lub upoważniona przez niego osoba ustala odrębny identyfikator oraz hasło dostępu do programu.

§3. Hasła użytkownika nie wolno nigdzie zapisywać, ani na papierze ani w formie elektronicznej-należy je zapamiętać. Hasła należy zmieniać co miesiąc.
Jako hasła nie należy używać żadnych wyrazów lub liczb występujących w danych personalnych użytkownika.

§ 4. Hasła użytkownika , umożliwiajace dostęp do systemu informatycznego, utrzymuje się w tajemnicy również po upływie ich ważności.

§ 5. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

§ 6. Identyfikator o którym mowa w § 2 , wpisuje się do ewidencji osób zatrudnionych przy ich przetwarzaniu wraz z imieniem i nazwiskiem użytkownika oraz rejestruje w systemie informatycznym.

§7. Identyfikatory użytkowników nie podlegają okresowym zmianom. Po wyrejestrowaniu użytkownika z systemu informatycznego ten sam identyfikator nie powinien być przydzielany innej osobie.

§8. Posługiwanie się danymi identyfikującymi należącymi do innego użytkownika w celu dostępu do systemu informatycznego lub podejmowanie jakichkolwiek innych działań w jego imieniu jest nielegalne również za zgodą właściwego użytkownika.

§9. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 10. Administrator bezpieczeństwa informacji jest odpowiedzialny za właściwy nadzór nad funkcjonowaniem mechanizmów, o których mowa w § 1-9.

III. Procedury rozpoczęcia i zakończenia pracy

§1. Pracownik uruchamiający pracę systemu przetwarzającego dane osobowe powinien upewnić się, że od czasu ostatniego zakończenia pracy nie nastąpiło naruszenie zabezpieczeń systemu, o którym mowa w § 6 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych , jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych(Dz.U. Nr 80, poz.521).

§2. W razie stwierdzenia lub uzasadnionego podejrzenia , że naruszenie miało miejsce, pracownik postępuje zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§3. Jeżeli użytkownik pracuje w sieci rejestruje się w systemie podając hasło sieciowe.

§4. Uruchomienie programu następuje po podaniu identyfikatora użytkownika i hasła.

§5. W przypadku kiedy użytkownik musi na krótko opuścić stanowisko pracy, powinien co najmniej zakończyć pracę programu aby uniemożliwić przeglądanie, ewentualnie wprowadzenie danych.

§6. Ustala się pomieszczenia o nr: 6, 6A, 7,9,10,11,12,13, jako tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

§7. Przebywanie wewnątrz obszaru o którym mowa w § 6 osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

§8. W pomieszczeniach w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób , by uniemożliwić tym osobom wgląd w dane. W razie krótkotrwałej przerwy w pracy ekran należy wygasić lub zastosować inne środki uniemożliwiające osobom postronnym wgląd w dane.

§9. Po zakończeniu pracy należy sprawdzić czy system został prawidłowo wyłączony oraz zastosować techniczne i organizacyjne środki zabezpieczenia ustalone na czas niedziałania systemu.

IV. Metoda i częstotliwość tworzenia kopii zapasowych.

§1.Kopie zapasowe obejmują kopie awaryjne oraz kopie bezpieczeństwa.

§2. Kopie awaryjne tworzy się poprzez dodatkowe zapisanie danych na nośniku komputerowym(dyskietce lub CD). Zapisu takiego dokonuje się raz na tydzień oraz przed każdym przeglądem lub konserwacją systemu.
Raz na tydzień dokonuje się zapisu danych na taśmy strimera.

§ 3. Kopie bezpieczeństwa zawierają programy komputerowe wykorzystywane w systemie przetwarzania danych osobowych. Kopie takie tworzy się tylko w przypadkach , w których jest to niezbedne dla funkcjonowania systemu. Kopie programów będących cudzą własnością, użytkowane w urzędzie na podstawie umowy licencyjnej lub podobnego tytułu prawnego, mogą być stosowane równocześnie z programem pierwotnym tylko wtedy, gdy umowa z właścicielem programu nie stanowi inaczej. Nie dotyczy to badania przydatności tych kopii, o którym mowa w § 5.

§4. Kopie zapasowe należy przechowywać w zamkniętych szafach zlokalizowanych w pomieszczeniach innych niż pomieszczenia , w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco, przez okres co najmniej 1 miesiąca.

§5. Przydatność kopii zapasowych do użytku, w szczególności pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu, należy sprawdzać co najmniej 1 raz na miesiąc.

§6. Kopie zapasowe nieprzydatne do użytku niszczy się poprzez usunięcie danych lub przez fizyczną kasację nośnika.

V . Sprawdzanie obecności i usuwanie wirusów komputerowych

§1. W celu wykrycia i usuwania wirusów komputerowych należy w systemie przetwarzania danych osobowych zainstalować odpowiednio dobrane programy antywirusowe.

§2. Badania antywirusowe przeprowadza się raz na miesiąc oraz niezwłocznie jeżeli podejrzewa się zawirusowanie komputera.

VI . Postępowanie ze sprzętem komputerowym i nośnikami danych.

§1. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną , powinny być zabezpieczone przed utratą tych danych spowodowaną utratą zasilania lub zakłóceniami w sieci zasilającej.

§2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

§3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.

§4. Urządzenia, dyski lub inne informatyczne nośniki danych , przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora bezpieczeństwa informacji.

§5. Nośniki informacji oraz wydruki zawierające dane osobowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.Wydruki przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§6. Z zastrzeżeniem § 7. , przenośny komputer służący do przetwarzania danych osobowych, może być w uzasadnionych przypadkach wyniesiony poza obszar obiektu, w którym są przetwarzane dane osobowe, za zezwoleniem administartora bezpieczeństwa informacji lub w razie jego nieobecności- kierownika urzędu.

§7. Wynoszenie komputera przenośnego poza obszar obiektu o którym mowa w §6 jest niedopuszczalne, jeżeli w komputerze tym przechowuje się informacje niejawne oznaczone klauzulą „poufne" lub „ zastrzeżone".

§8. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem o którym mowa w §6, w celu zapobieżenia dostępowi do tych danych osoby niepowołanej, a w szczególności powinna:

1) zabezpieczyć dostęp do komputera hasłem,
2) nie zezwalać na dostęp do komputera osobom nieupoważnionym do dostępu do danych osobowych.

VII. Przegląd i konserwacja systemów i zbioru danych osobowych.

§1. Przegląd i konserwacja systemów przetwarzania danych osobowych dokonuje się raz na rok, z zachowaniem warunków wynikających z umów zawartych w tym zakresie z kontrahentami urzędu.

VIII. Postanowienia końcowe

§1. Ewidencję osób zatrudnionych przy komputerowym przetwarzaniu danych osobowych i odpowiedzialnych za archiwizację prowadzi Administrator Bezpieczeństwa Informacji wg wzoru: imię i nazwisko, nazwa programu, uprawnienia, nazwa użytkownika sieci, referat , data dopuszczenia do przetwarzania danych, data cofnięcia uprawnień.

§2. Osoby wyznaczone do archiwizacji są odpowiedzialne za odnotowanie wszystkich wykonywanych czynności w „rejestrze wykonanych czynności".

§3. Przekazywanie informacji za pośrednictwem poczty elektronicznej, korzystanie z Internetu może odbywać się wyłącznie na stanowiskach nie związanych z przetwarzaniem danych osobowych.

WÓJT
Józef Caputa

Załącznik nr 3
do Zarządzenia Nr 10
Kierownika Urzędu Gminy Buczkowice
z dnia 30 czerwca 2003r.

Wzór oświadczenia pracownika
o znajomości przepisów z zakresu ochrony danych osobowych

Buczkowice, dnia.....

.....
imię i nazwisko pracownika

.....
komórka organizacyjna Urzędu

.....
stanowisko

OŚWIADCZENIE

Oświadczam ,że są mi znane przepisy ustawy z dnia 29 sierpnia1997r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn.zm.) oraz przepisy wykonawcze do tej ustawy, jak również Zarządzenie Nr 9 i 10 Kierownika Urzędu Gminy Buczkowice z dnia 30 czerwca 2003r. i że zobowiązuję się do ich stosowania i przestrzegania.

.....
podpis pracownika