Z A R Z Ą D Z E N I E Nr 187/2011

Wójta Gminy Celestynów
z dnia 26 września 2011 roku

w sprawie ustanowienia Polityki Bezpieczeństwa Urzędu Gminy Celestynów

Na podstawie art. art. 39 a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. z 2002 r, Nr 101, poz. 926 z późn. zm.) w związku z § 3 ust.1 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) **zarządzam**, co następuje:

§ 1

W celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Celestynów, ustanawia się Politykę Bezpieczeństwa, stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik
do Zarządzenia nr
187/2011
Wójta Gminy Celestynów
z dnia 26 września 2011 r.

Polityka Bezpieczeństwa
Urzędu Gminy Celestynów

§ 1.

1. Niniejszą Politykę Bezpieczeństwa Urzędu Gminy Celestynów opracowano i ustanowiono na podstawie:
1) art. 39 a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (j.t. Dz.U. z 2002 r, Nr 101, poz. 926 z późn. zm.);
2) 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. Ilekroć w dalszej części Polityki Bezpieczeństwa Urzędu Gminy Celestynów mowa jest o:
1) **Polityce bezpieczeństwa** - należy przez to rozumieć Politykę Bezpieczeństwa Urzędu Gminy Celestynów;
2) **Urzędzie** - należy przez to rozumieć Urząd Gminy Celestynów;
3) **Administrator Danych Osobowych (ADO) –** należy przez to rozumieć organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Wójt Gminy Celestynów, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego dyspozycji;
4) **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika Urzędu wyznaczonego przez Administratora Danych Osobowych do wdrażania oraz nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
5) **Administrator Systemu Informatycznego (ASI)** – należy przez to rozumieć pracownika lub pracowników firmy informatycznej wyznaczonej przez Administratora Danych Osobowych, odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych przetwarzanych w systemie informatycznym;
6) **Użytkownik** – należy przez to rozumieć osobę posiadająca upoważnienie wydane przez ADO do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu;
7) **Bezpośrednim przełożonym** - należy przez to rozumieć: w stosunku do osoby kierującej jednostką organizacyjną urzędu - wójta lub upoważnioną przez niego osobę, w stosunku do pozostałych pracowników - kierującego jednostką organizacyjną urzędu lub wskazaną w zakresie danych czynności pracownika osobę wyznaczoną do bezpośredniego nadzoru. W przypadku osoby upoważnionej do przetwarzania danych osobowych na podstawie innego niż zatrudnienie stosunku prawnego, bezpośrednim przełożonym jest osoba nadzorująca wykonywanie przez nią czynności ze strony Urzędu;

8) **Kodeksie pracy -** należy przez to rozumieć ustawę z dnia 26 czerwca 1974 roku Kodeks pracy (tekst jednolity: Dz. U. z 1998 roku, nr 21, poz. 94 z późn. zm.).

§ 2

Polityka bezpieczeństwa określa środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczności danych osobowych, przetwarzanych za pomocą systemu informatycznego w Urzędzie.

§ 3

Podmiotami odpowiedzialnymi za zgodne z prawem przetwarzanie danych osobowych są:
1) Administrator Danych Osobowych;
2) Administrator Bezpieczeństwa Informacji;
3) Administrator Systemów Informatycznych;
4) Użytkownik systemu, upoważniony do przetwarzania danych osobowych w Urzędzie na podstawie udzielonego upoważnienia, którego wzór stanowi załącznik nr 1 do Polityki bezpieczeństwa.

§ 4

1. Zasady określone w Polityce bezpieczeństwa, obowiązują wszystkich pracowników Urzędu bez względu na sposób nawiązania stosunku pracy, wymiar czasu pracy i zajmowane stanowisko.
2. Do ich przestrzegania są zobowiązane osoby, które uzyskały upoważnienie do przetwarzania danych osobowych, na podstawie innego niż zatrudnienie stosunku prawnego.
3. Osoby, o których mowa powyżej, są zobowiązane do złożenia stosownego oświadczenia, którego wzór stanowi załącznik nr 2 do Polityki bezpieczeństwa.

§ 5

Dane osobowe przetwarzane są w siedzibie Urzędu przy ulicy Reguckiej 3 w pomieszczeniach, w których znajdują się stanowiska komputerowe, a także serwer.

§ 6

Do przetwarzania danych osobowych w Urzędzie, wykorzystywane są następujące programy informatyczne:
1) Kancelaria;
2) Selwin;
3) Podatki;
4) JUG;
5) Księgowość;
6) Bestia;
7) Płatnik;
8) Budżet;
9) Kadry i Płace;
10) Środki trwałe;
11) Ewidencja ludności;
12) System obsługi USC;

13) System wydania dowodów osobistych;
14) Ewidencja działalności gospodarczej;
15) Ewidencja numeru budynków;
16) PEFS.

§ 7

1. Budynek Urzędu, w którym przetwarzane są dane osobowe, jest zabezpieczony systemem stałego monitoringu.
2. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami drzwiowymi, zaś klucze do pokoi wydawane są jedynie osobom upoważnionym.
3. Dostęp do pomieszczenia, w którym znajduje się serwer, zabezpieczony jest zamkiem drzwiowym. Serwer umieszczony jest w specjalnie przeznaczonej do tego szafie, zabezpieczonej przed dostępem osób nieupoważnionych zamkiem drzwiowym.
4. Zalogowanie do serwera wymaga podania nazwy użytkownika i hasła, zaś dostęp do stacji roboczych chroniony jest hasłem.
5. Wykorzystany jest system szyfrowania danych (dostępny w systemie operacyjnym) uniemożliwiający odczyt danych osobom nieupoważnionym.
6. W celu zabezpieczenia przed dostępem osób nieupoważnionych do baz danych za pośrednictwem sieci internet, zastosowano firewall.
7. Urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania. Zastosowano również ochronę z wykorzystaniem programu antywirusowego.
8. W celu zabezpieczenia się przed utratą danych wykonywane są kopie zapasowe.

§ 8

1. Użytkownicy przed przystąpieniem do pracy przy przetwarzaniu danych powinni zwrócić uwagę, czy nie istnieją przesłanki do tego, że dane zostały naruszone. Jeżeli istnieje takie podejrzenie, należy niezwłocznie zgłosić Administratorowi Bezpieczeństwa Informacji.
2. Dostęp do konkretnych zasobów danych jest możliwy dopiero po podaniu właściwego hasła dostępu.
3. Hasło użytkownika należy podawać do systemu w sposób dyskretny tzn. nie literować, nie czytać na głos, wpisywać osobiście.
4. Użytkownik ma obowiązek zamykania systemu, programu komputerowego po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem, programem nie może pozostawać bez kontroli pracującego na nim użytkownika.
5. Pomieszczenia, w których znajdują się urządzenia służące do przetwarzania danych oraz wydruki lub inne nośniki zawierające dane, pod nieobecność personelu muszą być zamknięte. Dostęp do nich mogą mieć jedynie osoby upoważnione.
6. Użytkownik jest zobowiązany do zachowania w tajemnicy danych osobowych, do których uzyskał dostęp w ramach przetwarzania danych osobowych, również po ustaniu zatrudnienia, jak i innego stosunku prawnego, będącego podstawą uzyskania upoważnienia do przetwarzania danych osobowych.
7. Na użytkowniku w trakcie przetwarzania danych osobowych, ciąży obowiązek nie dopuszczenia do ich udostępnienia podmiotom nieupoważnionym.

§ 9

Naruszeniem zasad ochrony danych osobowych jest ich przetwarzanie w sposób niezgodny z powszechnie obowiązującymi przepisami prawa, a także regułami określonymi w polityce bezpieczeństwa polegające w szczególności na:

1) nieupoważnionym dostępie, modyfikacji, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych przez podmioty nieupoważnione;
2) udostępnianie danych osobowych podmiotom nieupoważnionym;
3) nieautoryzowany dostęp do danych przez połączenie sieciowe;
4) dostęp do pomieszczeń, w których przetwarza się dane osobowe przez osoby nieuprawnione;
5) niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe);
6) obecność wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego;
7) ujawnienie indywidualnych haseł dostępu do systemu;
8) wykonanie nieuprawnionych kopii danych osobowych;
9) naruszenie bezpieczeństwa kopii danych osobowych;
10) kradzież nośników zawierających dane osobowe lub oprogramowanie;
11) kradzież sprzętu służącego do przetwarzania danych osobowych;
12) niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt;
13) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe.

§ 10

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad przetwarzania danych osobowych, w tym celu prowadzi dziennik (zwany dalej dziennikiem ABI), w którym zapisuje wszystkie informacje dotyczące naruszenia bezpieczeństwa informacji oraz podjęte w związku z tym działania.
2. W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych, użytkownik jest zobowiązany do natychmiastowego poinformowania o tym Administratora Bezpieczeństwa Informacji, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych Administratora Systemów Informatycznych (stosowny zapis w dzienniku ABI).
3. W przypadku niemożności poinformowania podmiotów, o których mowa w § 9 ust. 2, użytkownik jest zobowiązany powiadomić bezpośredniego przełożonego.
4. Gdy stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazać na naruszenie zabezpieczenia tych baz, to fakt ten należy zgłosić Administratorowi Bezpieczeństwa Informacji (stosowny zapis w dzienniku ABI).
5. Administrator Bezpieczeństwa Informacji razem z Administratorem Systemów Informatycznych usuwają przyczynę naruszenia systemu informatycznego, sprawdzają cały system i dokonują wpisu do dziennika ABI, a także wdrażają dodatkowe zabezpieczenia.
6. W sytuacjach, o których mowa w § 9 ust. 2 i 3 użytkownik dokonuje zgłoszenia na piśmie, powinno ono zawierać:

1) wskazanie osoby zgłaszającej, kiedy(data), o której godzinie;
2) na czym polega naruszenie ochrony danych osobowych;
3) zabezpieczone dowody naruszenia danych;

4) propozycje wniosków co do dalszego trybu postępowania, w tym dotyczących zmiany systemu ochrony danych.

7. Zgłoszenie, o którym mowa w ust. 6 przekazuje się niezwłocznie Administratorowi Bezpieczeństwa Informacji oraz Wójtowi.
8. Wójt wdraża postępowanie wyjaśniające. Jeżeli stwierdzone zostanie naruszenie ochrony danych osobowych z winy pracownika wszczyna się postępowanie z tytułu naruszenia obowiązków pracownika, na zasadach określonych w kodeksie.
9. W przypadku stwierdzenia, iż naruszenie ochrony danych wyczerpuje znamiona przestępstwa, sporządza się zawiadomienie do odpowiednich organów.

§ 11

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje Administrator Systemów Informatycznych.
2. Ocenie podlegają stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan zabezpieczeń fizycznych (zamki, kraty), stan rejestrów systemów serwera lokalnej sieci komputerowej.

§ 12

1. Użytkownicy systemu, będący pracownikami Urzędu za naruszenie reguł określonych w Polityce bezpieczeństwa, ponoszą odpowiedzialność z tytułu naruszenia obowiązków pracownika na zasadach określonych w Kodeksie.
2. Osoby nie będące pracownikami, ponoszą odpowiedzialność określoną na zasadach wynikających ze stosunku prawnego, będącego podstawą upoważnienia do przetwarzania danych osobowych.
3. Pociągnięcie do odpowiedzialności w sposób określony powyżej, nie wyklucza poniesienia odpowiedzialności karnej z tytułu naruszenia przepisów ustawy.

§ 13

1. Każdy nowoprzyjęty pracownik jest zapoznawany z treścią Polityki bezpieczeństwa i jest zobowiązany do jej przestrzegania.
2. W sprawach nieuregulowanych w Polityce bezpieczeństwa, zastosowanie mają powszechnie obowiązujące przepisy prawa.
3. Zmiany Polityki bezpieczeństwa są dokonywane w trybie, przewidzianym dla jej ustalenia.

Załącznik Nr 1
do „Polityki bezpieczeństwa
Urzędu Gminy Celestynów”

Celestynów, dnia …….....

**Upoważnienie imienne nr ……
do przetwarzania danych osobowych**

Na podstawie art. 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w/ wykonującą (ego) czynności na podstawie, innego niż zatrudnienie stosunku prawnego

.....

(nazwa jednostki i komórki organizacyjnej)

na stanowisku: ....

….

do przetwarzania od dnia .....20…..… r. danych osobowych w

zakresie .....

.....

…….
(podpis administratora danych osobowych)

Załącznik nr 2
do Polityki Bezpieczeństwa
Urzędu Gminy Celestynów

Celestynów, dnia .....

.....
(imię i nazwisko osoby)

.....
(stanowisko i nazwa komórki organizacyjnej)

O Ś W I A D C Z E N I E

Ja, niżej podpisana(y), oświadczam, że zapoznała(e)m się z przepisami dotyczącymi przetwarzania i ochrony danych osobowych i zobowiązuję się do ich przestrzegania w szczególności:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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),
3. Procedur dotyczących bezpieczeństwa przetwarzania i ochrony danych osobowych, określonych w zarządzeniach Wójta Gminy Celestynów.

Jednocześnie oświadczam, że:

1) zapewnię ochronę danym osobowym przetwarzanym w Urzędzie Gminy Celestynów, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
2) zachowam w tajemnicy, także po ustaniu stosunku pracy, innego niż zatrudnienie stosunku prawnego wszelkie informacje dotyczące przetwarzania oraz sposobów zabezpieczenia danych osobowych w Urzędzie Gminy Celestynów,
3) natychmiast zgłoszę przełożonemu i Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy Celestynów, stwierdzenie próby lub faktu naruszenia ochrony lub bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe.

.....
(podpis osoby upoważnionej do dostępu)

Oświadczenie wypełnia osoba, która wykonując swoje obowiązki musi posiadać dostęp do danych osobowych przetwarzanych w Urzędzie Gminy Celestynów. Oświadczenie jest zgodne z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)