

Zarządzenie 31 /06
Wójta Gminy Ciechocin
z dnia 19 października 2006 r.

w sprawie ustalenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ciechocin.

Na podstawie § 4 i § 5 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. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Ustalam politykę bezpieczeństwa ochrony przetwarzania danych osobowych w Urzędzie Gminy Ciechocin, stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ciechocin, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Pracownicy Urzędu Gminy Ciechocin zostaną zapoznani z załącznikami do niniejszego zarządzenia poprzez otrzymanie ich do wglądu lub skopiowania.

§ 2. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY
inż. Bronisław Jaskólski

Polityka bezpieczeństwa ochrony przetwarzania danych osobowych w Urzędzie Gminy Ciechocin.

§ 1. 1. Polityka bezpieczeństwa jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystaniu danych osobowych w Urzędzie Gminy. Dotyczy ona całego procesu korzystania z informacji, niezależnie od sposobu jej gromadzenia i przetwarzania.

2. Polityka bezpieczeństwa określa zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

§ 2. Polityka bezpieczeństwa służy do ochrony przed utratą następujących cech gromadzonych i przetwarzanych danych osobowych:

- 1) poufności – zapewniającej, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom;
- 2) integralności danych – zapewniającej, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 3) integralności systemu – polegającej na tym, że system realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej;
- 4) dostępności – właściwości bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
- 5) autentyczności – zapewniającej, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy: użytkowników, systemów i informacji;
- 6) niezawodności – właściwości oznaczającej spójne, zamierzone zachowanie i skutki.

§ 3. 1. Dane osobowe w Urzędzie Gminy Ciechocin w systemach informatycznych są przetwarzane w następujących pokojach:

- | | |
|--|-----------------|
| 1) Ewidencja ludności i dowody osobiste | - pokój Nr 10, |
| 2) Referat Finansowy – ewidencja opłat i podatków lokalnych | - pokój Nr 6, |
| 3) Gminny Zespół Ekonomiczno Administracyjny Szkół
– ewidencja danych osobowych odnoszących się do zatrudnienia pracowników szkół | - pokój Nr 5, |
| 4) Ewidencja danych osobowych odnoszących się do zatrudnienia pracowników urzędu | - pokój Nr 7- 9 |
| 5) Gminny Ośrodek Pomocy Społecznej
-ewidencja danych osobowych odnoszących się do zatrudnionych pracowników
-ewidencja danych osobowych osób korzystających z opieki społecznej.
-ewidencja danych osobowych korzystających z zasiłków rodzinnych. | - pokój Nr 4 |
| 6) Referat finansowy
– ewidencja danych osobowych pracowników UG
– ewidencja danych osobowych osób korzystających ze stypendium szkolnego. danych | - pokój Nr 2 |
| 10) Ewidencja danych osobowych w spr. zezwoleń na sprzedaż napojów alkohol. | - pokój nr 6 |
| 11) Ewidencja danych osobowych w spr. decyzji o warunkach zabul. i zagosp. terenu- | pokój Nr 1 |

2. Dane osobowe w Urzędzie Gminy Ciechocin bez użycia systemu informatyczne są przetwarzane w następujących pokojach:

- 1) Ewidencja opłat za dzierżawę i wieczyste użytkowanie- pokój Nr 1

- 2) Ewidencja zamówień publicznych
- 3) Ewidencja przedpoborowych i poborowych
- 4) Urząd Stanu Cywilnego
- 5) Ewidencja skarg i wniosków

- pokój Nr 1
- pokój Nr 10
- pokój Nr 10
- pokój Nr 7-9

§ 4. Do przetwarzania danych osobowych w systemach informatycznych wykorzystywane są następujące programy:

- 1) ewidencja opłat i podatków lokalnych – COM COM
- 2) ewidencja ludności – Aram Sp. z o.o. 1998 r.,
- 3) dowody osobiste – IDL-SYS,
- 4) ewidencja danych odnoszących się do zatrudnienia pracowników szkół – Kadry i Płace – Z. Chlebowski
- 5) ewidencja danych odnoszących się do zatrudnienia pracowników urzędu – Płatnik, Płace
- 6) ewidencja wypłacanych stypendia- SPUTNIK
- 7) ewidencja podatków i opłat – COM COM
- 8) księgowość podatkowa COM COM
- 9) ewidencja działalności gospodarczej SPUTNIK
- 10) ewidencja danych osobowych pracowników GOPS - Płace Optive Wulkan
- 11) ewidencja danych osobowych korzystających z opieki społecznej – POMOST
- 12) ewidencja danych osobowych korzystających z świadczeń rodzinnych – SPUTNIK
- 13) ewidencja danych osobowych korzystających zasiłków alimentacyjnych - SPUTNIK

§ 5. Dane zawarte zarówno w systemach informatycznych, jak również w kartotekach, rejestrach mogą być wykorzystywane wyłącznie zgodnie z ich przeznaczeniem do wykonywania zadań samorządu gminy określonych w przepisach prawa.

§ 6. 1. Dane osobowe mogą być zbierane i przetwarzane wyłącznie przez osoby posiadające ważne upoważnienie nadane przez Administratora Danych.

2. W Urzędzie Gminy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, którą prowadzi i aktualizuje pracownik do spraw organizacyjnych i kadr .

3. Osoby posiadające upoważnienia do przetwarzania danych osobowych składają oświadczenia o zapoznaniu się z przepisami i instrukcjami dotyczącymi ochrony danych osobowych oraz oświadczają, że zachowają znajomość tych danych w tajemnicy, będą je wykorzystywać wyłącznie do celów, dla których są one zbierane i nie będą ich udostępniać osobom nieupoważnionym.

4. Szczegółowe zakresy obowiązków każdego z pracowników określają zakres przetwarzanych przez nich danych osobowych oraz nakładają na nich obowiązek dbania o bezpieczeństwo powierzonego zasobu systemu informacyjnego, tj. sprzętu komputerowego, archiwum danych.

5. Dany zbiór danych osobowych jest przyporządkowany konkretnemu pracownikowi, zgodnie z ewidencją osób upoważnionych do przetwarzania danych osobowych. Przy przenoszeniu odpowiedzialności za konkretny zbiór danych następuje unieważnienie upoważnienia dla pracownika oraz nadanie upoważnienia kolejnemu pracownikowi.

§ 7. Dla kontroli poprawności przestrzegania zasad ochrony danych osobowych Administrator Danych wyznacza administratora bezpieczeństwa informacji. Do czasu jego powołania Administrator Danych sam wykonuje te czynności.

§ 8. 1. Dane osobowe zgromadzone w kartotekach i rejestrach znajdują się w zamykanych na zamki patentowe szafkach oraz w sejfach, do których dostęp mają wyłącznie osoby posiadające upoważnienie do przetwarzania określonych danych osobowych.

2. Szafy, sejfy w których przechowywane są dane osobowe znajdują się w pomieszczeniach zamykanych na zamki patentowe oraz na parterze budynku w okratowane okna.

3. Budynek Urzędu gminy jest chroniony podwójnymi, antywłamaniowymi drzwiami. Budynek nie jest obiektem chronionym po przez zainstalowanie systemu alarmowego.

4. Pomieszczenia, w których są przetwarzane dane osobowe, na czas nieobecności w nich osób upoważnionych do przetwarzania danych, muszą być zamykane w sposób uniemożliwiający wejście do nich osób nieupoważnionych.

5. Wprowadzanie nowych danych, zmian i aktualizacji do rejestrów i kartotek zawierających dane osobowe może być dokonywane tylko przez osobę upoważnioną do prowadzenia tego rejestru w sposób dający się zidentyfikować poprzez składanie podpisu.

§ 9. 1. Dane osobowe zgromadzone w systemach informatycznych są chronione przez system identyfikatorów i haseł znanych osobom upoważnionym do przetwarzania danych oraz administratorowi sieci. Zasady nadawania, unieważniania haseł zostały określone w *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ciechocin*.

2. W Urzędzie Gminy wprowadza się zakaz używania oprogramowania innego niż oficjalnie zakupione i dopuszczone do używania przez administratora sieci.

3. Każda pojedyncza dyskietka, dysk lub inny nośnik informacji niewiadomego pochodzenia powinna bezwzględnie zostać sprawdzona licencjonowanym oprogramowaniem antywirusowym przed jej wykorzystaniem. Pracownicy powinni dążyć w miarę możliwości do wyeliminowania potrzeby korzystania z dyskietek lub innych tego typu wymiennych nośników danych.

4. Osoby odpowiedzialne za utrzymanie systemu informacyjnego mają prawo i obowiązek do regularnych inspekcji systemu w poszukiwaniu danych lub oprogramowania niewiadomego pochodzenia, a mogących wpłynąć na obniżenie poziomu bezpieczeństwa systemu informacyjnego.

§ 10. Procedura postępowania w razie wystąpienia naruszenia danych osobowych lub podejrzenia takiego naruszenia została opisana w *Instrukcji postępowania w sytuacji naruszenia danych osobowych*.

§ 11. Polityka bezpieczeństwa ochrony przetwarzania danych osobowych w Urzędzie Gminy Ciechocin jest dokumentem obowiązującym wszystkich zatrudnionych w Urzędzie pracowników oraz podmiotów zewnętrznych współpracujących z Urzędem.

WÓJT GMINY
inż. Bronisław Jaskólski

*Załącznik nr 2
do Zarządzenia Nr 31/06
Wójta Gminy Ciechocin
z dnia 19 października 2006 r.*

**Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych
osobowych w Urzędzie Gminy Ciechocin.**

§ 1. Każdy ma prawo do ochrony dotyczących go danych osobowych.

§ 2. Za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.

§ 3. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
- 2) zezwalają na to przepisy prawa,
- 3) jest niezbędne dla osoby, której dane dotyczą, w celu wywiązania się z umowy, której jest stroną lub na jej życzenie w celu podjęcia niezbędnych działań przed zawarciem umowy,
- 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- 5) jest niezbędne do wypełnienia usprawiedliwionych celów administratorów danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

§ 4. Z uwagi na ochronę interesów osób, których dane dotyczą, zapewnia się:

- 1) przetwarzanie danych zgodnie z prawem,
- 2) zbieranie danych dla oznaczonych zgodnie z prawem celów i nie poddawanie ich dalszemu przetwarzaniu niezgodnemu z tymi celami,
- 3) poprawność merytoryczną danych i ich adekwatność w stosunku do celów, w jakich są przetwarzane,
- 4) przechowywanie danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 5. Ustala się, że w Urzędzie Gminy Ciechocin obszarem, w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego są następujące pokoje:

- | | |
|--|---------------|
| 5) Ewidencja ludności i dowody osobiste | - pokój Nr 10 |
| 6) Referat Finansowy – ewidencja opłat i podatków lokalnych | - pokój Nr 6 |
| - ewidencja zezwoleń na sprzedaż napojów alkoholowych | |
| 7) Gminny Zespół Ekonomiczno Administracyjny Szkół | - pokój Nr 5 |
| - ewidencja danych osobowych odnoszących się do zatrudnienia pracowników szkół | - pokój Nr 5 |
| 8) Ewidencja danych osobowych odnoszących się do zatrudnienia pracowników urzędu | - pokój Nr 2 |
| 9) Gminny Ośrodek Pomocy Społecznej | - pokój Nr 4 |
| -ewidencja zatrudnionych pracowników , | |

- ewidencja osób korzystających z opieki społecznej,
- ewidencja osób korzystających ze świadczeń rodzinnych,
- ewidencja osób korzystających z zasiłku alimentacyjnego

10) Ewidencja przyznawania stypendium szkolnego

- pokój Nr 2

§ 6. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych.

§ 7. Wewnątrz obszaru, o którym mowa w § 5 osoby postronne mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych osobowych.

§ 8. Pomieszczenia, w których są przetwarzane dane osobowe, na czas nieobecności w nich osób upoważnionych do przetwarzania danych, muszą być zamykane w sposób uniemożliwiający dostęp do nich osób postronnych. Urządzenia i systemy informatyczne służące przetwarzaniu danych osobowych, zasilanie energią elektryczną muszą być przez cały czas zabezpieczone przed utratą tych danych, spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.

§ 9. 1. Każda osoba korzystająca z systemu informatycznego przetwarzania danych osobowych otrzymuje swój identyfikator oraz hasło.

2. Hasło jest unikalne, inne dla każdej osoby, zawiera minimum sześć znaków, jest nadawane przez administratora sieci i jest ważne przez jeden miesiąc.

3. Osobę, która utraciła uprawnienia dostępu do danych osobowych, należy niezwłocznie wyrejestrować, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

4. Po zakończeniu pracy programy powinny być wyłączone tak, aby osoby nieupoważnione nie mogły odczytać informacji z monitora komputera.

§ 10. Dostęp do istniejących programów zawierających dane osobowe w poszczególnych referatach Urzędu Gminy zostaje ograniczony do funkcji osoby korzystającej z danych osobowych, a wynikających z je zakresu obowiązków.

§ 11. 1. Administrator sieci tworzy raz w tygodniu kopie awaryjne, sprawdzając je równocześnie co miesiąc pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu. Po ustaniu użyteczności kopie awaryjne powinny być bezzwłocznie usuwane. Kopie są wykonywane jednym z dostępnych na rynku popularnych programów archiwizujących zabezpieczonych hasłem.

2. Kopie awaryjne są przechowywane w pokoju administratora w zamkniętej na klucz patentowy szafce.

§ 12. Sieć komputerowa jest co tydzień sprawdzana licencjonowanym programem antywirusowym. Tym samym programem sprawdzane są też drogi dostępu wirusów do sieci komputerowej, np. dyskietki.

§ 13. Konserwacje i przeglądy odbywają się przy wyłączonych komputerach tak, aby zgromadzone dane nie zostały zniszczone lub odczytane przez niepowołane osoby.

§ 14. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym system zapewnia odnotowanie:

- 1) daty pierwszego wprowadzenia danych do systemu,
- 2) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
- 3) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy z dnia 29 sierpnia 1997 r. O ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), którym dane osobowe zostały

udostępnione, dacie i zakresie tego udostępnienia,
4) sprzeciwu, o którym mowa w art. 32 ust.1 pkt 8 ustawy o ochronie danych osobowych.

2. Odnotowanie informacji, o których mowa w ust. 1 następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

§ 15. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkownika oraz kontroli dostępu do danych osobowych, w które wyposażony jest system informatyczny przetwarzający dane osobowe, sprawuje Administrator Danych.

WÓJT GMINY
inż. Bronisław Jaskólski