

Zarządzenie Nr 6/2000

Starosty Nowodworskiego

z dnia 25.02.2000r.

w sprawie wprowadzenia Instrukcji określającej sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w formie elektronicznej.

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998r. o Samorządzie Powiatowym (Dz. U. Nr 91, poz. 578 z póź. zmianami), w związku z § 6 i § 11 rozporządzenia MSWiA z dnia 3 czerwca 1998r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych (Dz. U. Nr 80, poz. 521) – **zarządza się:**

§ 1

Wprowadza się w Starostwie Powiatowym w Nowym Dworze Gdańskim Instrukcję w sprawie zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w formie elektronicznej, stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Odpowiedzialnym za wykonanie Zarządzenia i przestrzeganie wprowadzonej Instrukcji czyni się Kierowników Wydziałów Starostwa, Samodzielne stanowiska pracy oraz administratora bezpieczeństwa informacji – każdego w swoim zakresie.

§ 3

Nadzor nad wykonaniem Zarządzenia powierza się Sekretarzowi Powiatowemu.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
mgr Romuald Drynko

INSTRUKCJA

określająca sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w formie elektronicznej.

I. Postanowienia ogólne.

§ 1.

Podstawę prawną do niniejszej instrukcji stanowi: Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. (Dz. U. Nr 80, poz. 521, 522) oraz ustawa z dnia 22 stycznia 1999r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz.95) wraz z aktami wykonawczymi do obu ustaw.

§ 2.

Ilekróć w niniejszej instrukcji jest mowa o:

1. **danych osobowych** – należy przez to rozumieć każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby,
2. **systemach informatycznych** – należy przez to rozumieć użytkowane w Starostwie Powiatowym w Nowym Dworze Gdańskim informatyczne systemy służące do przetwarzania danych osobowych wraz z zasobami technicznymi i finansowymi i związanymi z dostarczaniem i rozprowadzaniem informacji,
3. **zabezpieczeniu systemu informatycznego** – należy przez to rozumieć zespół stosowanych środków technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed ujawnieniem, zniszczeniem, utratą, a także nieuprawnionym dostępem lub modyfikacją,
4. **administratorze danych** – należy przez to rozumieć osobę decydującą o celach i środkach przetwarzania danych osobowych,
5. **pełnomocniku ochrony** - należy przez to rozumieć osobę, do zadań której należy m.in. prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu informacji zawierających dane osobowe,
6. **administratorze bezpieczeństwa informacji** - należy przez to rozumieć osobę wyznaczoną przez administratora danych odpowiedzialnością za bezpieczeństwo danych, w tym szczególnie za przeciwdziałanie dostępowi do systemu osób niepowołanych oraz za podejmowanie działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
7. **administratorze systemu** - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego oraz techniczne wdrożenie systemu zabezpieczeń,
8. **użytkownika systemu informatycznego** - należy przez to rozumieć osobę upoważnioną i wyznaczoną przez administratora bezpieczeństwa informacji lub osobę uprawnioną, do przetwarzania danych osobowych i odpowiedzialną za ochronę danych na określonym stanowisku pracy.

§ 3.

1. Podstawowe zasady przetwarzania danych osobowych i zasady ochrony dostępu do danych osobowych są określone w Instrukcji w sprawie ochrony danych osobowych i sposobów postępowania w przypadkach jej naruszenia i są one obowiązujące dla tej instrukcji.
2. Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych, w tym szczególnie zasady ochrony,
3. Dane osobowe są informacjami niejawnymi, które wymagają ochrony przed nieuprawnionym dostępem, niezależnie od formy i sposobu ich wyrażania oraz niezależnie od zaklasyfikowania ich jako stanowiące tajemnicę służbową,
4. Organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych (GIODO),
5. Zbiory danych osobowych podlegają rejestracji przez GIODO, a zmiany odnośnie zakresu, celu, sposobu zbierania i udostępniania danych podlegają zgłoszeniu.

II. Zasady ogólne zarządzania systemem informatycznym.

§ 4.

1. System informatyczny służący do przetwarzania danych osobowych powinien mieć udokumentowane wszystkie jego elementy składowe i posiadać akceptację administratora systemu upoważniającą do funkcjonowania systemu.
2. Osoba pełniąca funkcję administratora systemu informatycznego winna posiadać upoważnienie administratora danych oraz akceptację administratorów bezpieczeństwa informacji.
3. Administrator systemu prowadzi ewidencję urządzeń wchodzących w skład systemu informatycznego.
4. Administrator systemu jest odpowiedzialny za opracowanie i aktualizowanie szczegółowej instrukcji zasad funkcjonowania, a szczególnie ochrony powierzonego mu systemu informatycznego, a w szczególności metod i częstotliwości sprawdzania wirusów komputerowych i metod ich usuwania, którą w jednym egzemplarzu przekazuje administratorowi bezpieczeństwa informacji oraz pełnomocnikowi ochrony.

§ 5.

1. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres zadań oraz odpowiedzialności tej osoby za ochronę danych przed niepowołanym dostępem, nielegalnym ujawnieniem lub pozyskaniem.
2. Każda osoba zatrudniona przy przetwarzaniu danych powinna być zaznajomiona z przepisami o ochronie danych osobowych oraz z przepisami o ochronie informacji niejawnych, co zostaje przez nią potwierdzone na stosownym „Oświadczeniu” (wzór oświadczenia stanowi załącznik nr 1).
3. Przebywanie w pomieszczeniach osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora bezpieczeństwa informacji.

§ 6.

1. Ekran monitorów poszczególnych stanowisk dostępu do danych osobowych winny być automatycznie wyłączane po upływie możliwie najkrótszego czasu nieaktywności użytkownika.
2. Monitory stanowisk dostępu do danych osobowych powinny być tak ustawione, aby uniemożliwić osobom postronnym przebywającym w pomieszczeniu wglądu do tych danych.

§ 7.

1. Informacje jednostkowe, wykazy i wydruki imienne, zestawienia zbiorcze lub inne dane z systemów zawierających dane osobowe mogą być wykonywane wyłącznie na pisemny wniosek zaakceptowany przez administratora bezpieczeństwa informacji.
2. Wydruki z systemów zawierające dane osobowe oraz inne nośniki informacji muszą być zabezpieczone do czasu ich odbioru przez zlecającego pracę.
3. Dyski, urządzenia, wydruki i maszynowe nośniki informacji przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych lub uszkadza w sposób uniemożliwiający ich odczytanie.

§ 8.

Kopie awaryjne tworzy się poprzez zapis na dysku zapasowym nie rzadziej niż raz na kwartał i przechowuje w zabezpieczonych pomieszczeniach innych niż te, w których przechowuje się zbiory danych wykorzystywanych na bieżąco, wskazanych przez administratora bezpieczeństwa informacji wydziału, w którym tworzy kopię.

§ 9.

Nośniki informacji, w tym kopie informatyczne oraz wydruki przechowywane są zgodnie z kategorią archiwalną, określoną w jednolitym wykazie akt.

III. Określenie sposobu identyfikacji użytkowników systemu informatycznego służącego do przetwarzania danych osobowych.

§ 10.

1. Dla każdego użytkownika systemu informatycznego w Starostwie w każdym wydziale, w którym przetwarza się informacje zawierające dane osobowe, administrator systemu z upoważnienia Kierownika Wydziału, ustala odrębny identyfikator i hasło (wzór upoważnienia stanowi załącznik nr2).
2. Identyfikator wpisuje się do ewidencji oraz rejestruje w systemie informatycznym.
3. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym powinien nastąpić po podaniu identyfikatora lub właściwego hasła.

identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie należy go przydzielać innej osobie oraz zabezpieczyć w taki sposób, aby uniemożliwić dalszy dostęp wyrejestrowanego użytkownika do danych.

5. Zmiana haseł dla użytkownika systemu w każdym Wydziale, w którym przetwarza się informacje zawierające dane osobowe – następuje raz w miesiącu i dokonywana jest przez administratora systemu, po uzyskaniu akceptacji właściwego Kierownika Wydziału.
6. Hasła umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy, również po upływie ich ważności.

IV. Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 11.

1. Ewidencję osób zatrudnionych przy przetwarzaniu informacji zawierających dane osobowe prowadzi pracownik Wydziału Organizacyjnego – pełnomocnik ochrony, na podstawie zgłoszeń do ewidencji, dokonywanych przez Kierowników Wydziałów, w których przetwarzane są informacje zawierające dane osobowe.
2. Ewidencja opatrzona jest klauzulą „poufne”.
3. Ewidencja powinna zawierać:
 - a) imię i nazwisko osoby zatrudnionej przy przetwarzaniu danych,
 - b) dane i kolejny numer upoważnienia,
 - c) identyfikator (mechanizm uwierzytelnienia użytkownika),
 - d) daty zmiany przydzielonego hasła.

V. Postępowanie w przypadkach naruszenia zabezpieczenia ochrony danych osobowych w systemie informatycznym.

§ 12.

1. W przypadku stwierdzenia uszkodzenia zabezpieczenia systemu informatycznego lub jeżeli stan urządzenia, zawartość zbioru danych lub sposób działania programu mogą wskazywać na naruszenie zabezpieczenia danych, osoba przetwarzająca dane osobowe niezwłocznie powiadamia o tym fakcie administratora bezpieczeństwa informacji – Kierownika właściwego Wydziału lub osobę przez niego upoważnioną (wzór upoważnienia stanowi załącznik nr 3).
2. Naprawa urządzeń lub innych informatycznych nośników zawierających dane osobowe może być dokonywana przez firmę na zlecenie Starostwa wyłącznie w obecności osoby zatrudnionej przy przetwarzaniu tych danych oraz pod bezpośrednim nadzorem Kierownika właściwego Wydziału lub administratora systemu.
3. W przypadku braku możliwości zapewnienia nadzoru, o którym mowa w ust.2. – należy urządzenia, dyski i inne informatyczne nośniki zawierające dane osobowe pozbawić zapisu takich danych.

VI. Postanowienia szczególne.

§ 13.

1. Czynności polegające na przetwarzaniu informacji zawierających dane osobowe mogą być wykonywane w godzinach pracy Starostwa Powiatowego w Nowym Dworze Gdańskim tj. od poniedziałku do piątku w godzinach od 7.³⁰ do 15.³⁰.
2. Wykonywanie czynności, o których mowa w ust.1 poza godzinami pracy Starostwa, wymaga zgody Starosty lub Sekretarza Powiatu.

§ 14.

Kierownik każdego Wydziału, w którym przetwarzane są informacje zawierające dane osobowe, odpowiada za sposób przetwarzania tych informacji, ustala częstotliwość wykonywania kopii awaryjnych, czasokres ich przechowywania oraz należyte zabezpieczenie danych przed dostępem osób postronnych oraz za zgłaszanie na bieżąco do ewidencji wymaganych niniejszą instrukcją informacji i danych związanych z przetwarzaniem informacji zawierających dane osobowe.

§ 15.

Kierownicy Wydziałów, w których przetwarza się informacje zawierające dane osobowe winni korzystać z systemu informatycznego i czuwać nad nim w taki sposób, aby dla każdej osoby, której dane są przetwarzane w systemie informatycznym możliwe było odnotowanie:

- 1) daty pierwszego wprowadzenia danych tej osoby,
- 2) źródła pochodzenia danych,
- 3) identyfikatora użytkownika wprowadzającego dane,
- 4) informacji – komu, kiedy i w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych innym podmiotom,
- 5) sprzeciwu osoby odnośnie przetwarzania jej danych.

oraz aby możliwe było udostępnianie na piśmie (w przypadkach przewidzianych przepisami prawa) treści danych o każdej osobie, której dane są przetwarzane wraz z wyżej wymienionymi informacjami dotyczącymi tej osoby.

§ 16.

Przeglądu oraz konserwacji sprzętu i aplikacji informatycznych w Wydziałach, w których przetwarzane są informacje zawierające dane osobowe – dokonuje informatyk w obecności osoby zatrudnionej przy przetwarzaniu danych.

VII. Postanowienia końcowe.

§ 17.

Udostępnianie danych osobowych innym podmiotom, może nastąpić tylko na pisemny wniosek (wzór wniosku stanowi Załącznik Nr 4) w przypadkach i w formie przewidzianych przepisami prawa.

§ 18.

Wszystkie osoby i firmy mające dostęp do zbioru danych w Starostwie Powiatowym w Nowym Dworze Gdańskim, zobowiązane są do podpisania oświadczeń o zachowaniu w tajemnicy wszelkich informacji i wiadomości jakie zostały ujawnione w związku z wykonywanymi czynnościami urzędowymi lub w związku z wykonywaniem przeglądów, konserwacji, napraw i usuwania awarii systemu oraz sprzętu informatycznego – w toku wykonywania tych czynności (wzór oświadczenia stanowi Załącznik Nr 5).

§ 19.

Postanowienia niniejszej instrukcji wchodzi w życie z dniem 25.02, 2000 roku.

Sporządził: Piotr Szmidtke

STAROSTA
mgr Edward Drynko

Wznowiono pod

tytuł. pi. w tym

RADCA PRAWNY

mgr Bogdan Bielawski
nr rej. Gd. E 194