OR.120.4.2011

Zarządzenie Nr 4/2011
Starosty Tarnobrzeskiego
z dnia 7 marca 2011 r.

w sprawie: ochrony danych osobowych w Starostwie Powiatowym w Tarnobrzegu

Na podstawie art. 32.ust.1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz.U.2001, Nr 142 poz. 1592 z późn. zm.) art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i 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

1. Wprowadza się ,,politykę bezpieczeństwa przetwarzania danych osobowych" w Starostwie Powiatowym w Tarnobrzegu stanowiącą załącznik Nr 1 do zarządzenia.
2. Wprowadza się Instrukcję zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego w Starostwie Powiatowym w Tarnobrzegu stanowiącą załącznik Nr 2 do zarządzenia.

§ 2

Jako Administrator danych osobowych ustanawiam:

1. Pełnomocnika Starosty ds. ochrony danych osobowych, sprawującego ogólny nadzór nad ochroną danych osobowych, organizacją ich przetwarzania, archiwizacją, udostępnianiem, rejestracją zbiorów danych oraz kontrolą w tym zakresie - Sekretarza Powiatu.
2. Administratora bezpieczeństwa informacji - pracownika odpowiedzialnego za zabezpieczenie systemu informatycznego tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochronę przed nieupoważnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem lub pozyskaniem danych osobowych i ich utratą oraz podejmowanie odpowiednich działań w przypadku naruszenia systemu informatycznego -Informatyka.

§ 3

1. Traci moc Zarządzenie Nr 10 Starosty Tarnobrzeskiego z dnia 2 września 1999 r. w sprawie organizacji ochrony danych osobowych w Starostwie Powiatowym w Tarnobrzegu.
2. Traci moc Zarządzenie Nr 11 Starosty Tarnobrzeskiego z dnia 10 września 1999 r. w sprawie wprowadzenia instrukcji dotyczącej ochrony danych osobowych w Starostwie Powiatowym w Tarnobrzegu oraz sposobu postępowania w przypadku jej naruszenia.

§ 4

Zarządzenie wchodzi w życie po upływie 14 dni od daty zapoznania się z treścią zarządzenia przez pracowników Starostwa.

Załącznik Nr 1
do Zarządzenia Nr 4/2011
Starosty Tarnobrzeskiego z dnia 7 marca 2011 r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Tarnobrzegu

I. Wstęp:

Celem Polityki bezpieczeństwa przetwarzania danych osobowych jest zabezpieczenie przetwarzania informacji stanowiących dane osobowe w rozumieniu ustawy o ochronie danych osobowych.

II. Obszar przetwarzania danych osobowych:

1. Obszar przetwarzania danych osobowych stanowi siedziba Starostwa Powiatowego (budynki administracyjne a w nich pomieszczenia, w których przetwarzane są dane osobowe, z użyciem sprzętu komputerowego lub w formie kartotek, ksiąg, map, skorowidzów i innych zbiorów ewidencyjnych.(Wydział Geodezji i Gosp. Gruntami, Wydział Komunikacji i Transportu, Wydział Budżetu i Finansów p.56, Wydział Organizacyjno Administracyjny p.38, Wydział Ochrony Środowiska , Rolnictwa i Leśnictwa, Referat Architektury i Budownictwa, Powiatowe Centrum Pomocy Rodzinie.)
2. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostanie się do środka osób niepowołanych.
3. W pomieszczeniach, w których przetwarza się dane osobowe, osoby trzecie mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych.
4. W pomieszczeniach, w których mogą przebywać osoby trzecie, monitory stanowisk dostępu do danych powinny być ustawione tak, aby uniemożliwiały wgląd w dane osobom nieupoważnionym.

III. Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania tych danych.

1. Ewidencja gruntów i budynków, 2. Ewidencja gruntów i budynków - ośrodek, 3.opinie do projektów sieci uzbrojenia terenu, 4. ewidencja pojazdów, ewidencja kierowców, 5.rejestr osób ubiegających się o umieszczenie w DPS, rodzin zastępczych, osób ubiegających się o ustalenie stopnia niepełnosprawności, 6. ochrona gruntów rolnych i leśnych, zwrot działek używanych dożywotnio, 7. ewidencja poborowych, 8. repatrianci, sprzedaż i użytkowanie wieczyste gruntów, przekształcenie prawa użytkowania wieczystego osobom fizycznym w prawo własności, wywłaszczenie i zwrot wywłaszczonych nieruchomości, 9. ewidencja pozwoleń na budowę i innych tworzonych na podstawie ustawy prawo budowlane, 10. licencje transportowe i inne uprawnienia transportowe, 11.zezwolenia dla stacji kontroli pojazdów oraz uprawnienia diagnostów, 12.zezwolenia dla szkół kierowców oraz uprawnienia instruktorów nauki jazdy, 13. rejestr kart wędkarskich i sprzętu pływającego
Zastosowane programy: VEGA, Ośrodek, Kierowca - MSWiA, CDN OPTIMA.

IV. Struktura zbioru danych

Zbiory danych w strukturze występują w układzie tabelarycznym, alfabetycznym lub wg kolejności numerów.

V. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Systemy nie są ze sobą zintegrowane. Nie są połączone siecią teleinformatyczną

VI. Środki techniczne i organizacyjne niezbędne dla zapewnienia bezpieczeństwa przetwarzania danych:

1. Środki ochrony fizycznej:
   a) budynek w którym zlokalizowany jest obszar przetwarzania danych osobowych w dni świąteczne i wolne od pracy oraz po godzinach urzędowania zabezpieczony jest przez ochronę fizyczną.
   b) urządzenia służące do przetwarzania danych osobowych znajdują się w zamkniętych pomieszczeniach.
   c) wejście do budynku ma podwójne drzwi i jest zamykane.
   d) pomieszczenia na parterze gdzie przetwarza się dane osobowe wyposażone są w okna zabezpieczone kratami.
   e) drzwi do pokoi zamykane są na zamki.

2. Środki organizacyjne:
   a) Pełnomocnik ds. ochrony danych osobowych prowadzi ewidencję osób dopuszczonych do przetwarzania danych osobowych.
   b) osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do przetwarzania danych podpisują:
      - upoważnienie do przetwarzania danych osobowych (zał. nr 1),
      - oświadczenie o znajomości przepisów dotyczących przetwarzania danych osobowych (zał. nr 2),
      - oświadczenie o zapoznaniu się z Instrukcją zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego. (zał. nr 3),

Załącznik Nr 1
do „Polityki Bezpieczeństwa”

UPOWAŻNIENIE Nr

Upoważniam .....do przetwarzania danych osobowych w zbiorze....
Upoważnienie jest ważne na czas...

.....
Starosta lub pełnomocnik Starosty

Pouczenie:
Osoba upoważniona obowiązana jest do zachowania w tajemnicy informacji uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych.(także po ustaniu zatrudnienia)

Przyjęłam/em do wiadomości i stosowania

.....
data i podpis pracownika

Załącznik Nr 2
do „Polityki Bezpieczeństwa”

OŚWIADCZENIE

Ja niżej podpisana(y) .....urodzona(y) ..... oświadczam, że znane mi są przepisy dotyczące przetwarzania danych osobowych.

.....
Starosta lub pełnomocnik Starosty

.....
data i podpis składającego oświadczenie

Załącznik Nr 3
do „Polityki Bezpieczeństwa”

OŚWIADCZENIE

Ja niżej podpisana(y) .....urodzona(y) .....
oświadczam, że zapoznałam(em) się z Instrukcją zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.

.....
Starosta lub pełnomocnik Starosty

.....
data i podpis składającego oświadczenie

Załącznik Nr 2
do Zarządzenia Starosty Tarnobrzeskiego Nr 4/2011
Starosty Tarnobrzeskiego z dnia 7 marca 2011 r.
w sprawie: ochrony danych osobowych w Starostwie Powiatowym w Tarnobrzegu

Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.

Postanowienia ogólne

§ 1

1. Przetwarzanie informacji, zawierających dane osobowe może się odbywać zgodnie z ustawą o ochronie danych osobowych oraz wydanymi na jej podstawie aktami normatywnymi.
2. Określony w niniejszej instrukcji tryb postępowania obowiązuje wszystkich pracowników Starostwa Powiatowego w Tarnobrzegu i kierowników jednostek organizacyjnych Powiatu, zatrudnionych przy przetwarzaniu danych osobowych lub których ochrona danych osobowych w jakimkolwiek stopniu dotyczy.

Podstawowe pojęcia

§ 2

1. Administrator danych - osoba decydująca o celach i środkach przetwarzania danych - Starosta Tarnobrzeski.
2. Pełnomocnik Starosty ds. ochrony danych osobowych, sprawujący ogólny nadzór nad ochroną danych osobowych, organizacją ich przetwarzania, archiwizacją, udostępnianiem, rejestracją zbiorów danych oraz kontrolą w tym zakresie - Sekretarz Powiatu.
3. Administrator bezpieczeństwa informacji - pracownik odpowiedzialny za zabezpieczenie systemu informatycznego tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochronę przed nieupoważnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem lub pozyskaniem danych osobowych i ich utratą oraz podejmowanie odpowiednich działań w przypadku naruszenia systemu informatycznego - Informatyk.

Zabezpieczenie danych osobowych

§ 3

Ochrona obszaru przetwarzania danych osobowych:

1) Przetwarzanie danych jest możliwe tylko przez uprawnione osoby w wyznaczonym przez administratora danych obszarze.
2) Przebywanie wewnątrz obszaru danych osobowych, osób nie uprawnionych do dostępu jest dopuszczalne tylko za zgodą administratora danych lub osoby przez niego upoważnionej.
3) Budynki i pomieszczenia, w których przetwarzane są dane osobowe muszą być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych, w sposób uniemożliwiający dostęp do nich osób niepowołanych i poddane szczególnej ochronie.
4) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Zabezpieczenie urządzeń i systemów informatycznych przed utratą danych osobowych lub dostępem osób niepowołanych:

1) Zabezpieczenie budynków urządzeniem „antyprzepięciowym" oraz zastosowanie zasilaczy awaryjnych (UPS) w celu zabezpieczenia przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2) Naprawa dysków lub innych informatycznych nośników zawierających dane osobowe powinna odbywać się w obecności i pod bezpośrednim nadzorem osoby upoważnionej przez administratora danych.
3) W przypadku braku możliwości zapewnienia nadzoru, o którym mowa w pkt. 2 należy urządzenia, dyski zawierające dane osobowe pozbawić zapisu tych danych.
4) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, a przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych lub uszkadza w sposób uniemożliwiający ich odczytanie.
5) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, a przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
6) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
7) Ekrany monitorów poszczególnych stanowisk dostępu do danych osobowych winny być automatycznie wyłączane po upływie możliwie najkrótszego czasu nieaktywności użytkownika. Monitory dostępu do danych osobowych powinny być tak ustawione, aby uniemożliwić osobom postronnym, przebywającym w pomieszczeniach wgląd do tych danych.
8) W przypadku użytkowania przenośnego komputera, służącego do przetwarzania danych, należy zabezpieczyć dostęp do tego komputera hasłem i nie zezwalać na użytkowanie go osobom niepowołanym.

Profilaktyka antywirusowa:

1) Każdy przenośny nośnik informacji elektronicznej wprowadzony do stacji dysków musi być uprzednio skontrolowany programem antywirusowym - dostępnym u administratora bezpieczeństwa informacji. Dotyczy to także kopii archiwalnych.

2) Nie rzadziej niż raz w miesiącu wszystkie samodzielne stanowiska komputerowe oraz serwer sieciowy należy sprawdzić aktualnym programem antywirusowym.*

(* zalecenie dot. serwera sieciowego obowiązywać będzie z chwilą jego instalacji)

3) Instalacji oprogramowania na dyskach twardych komputerów lub w sieci dokonuje administrator bezpieczeństwa informacji lub firma w jego obecności. Zabronione jest samodzielne instalowanie jakiegokolwiek oprogramowania za wyjątkiem sterowników (driverów) posiadanego sprzętu.

4) Konserwacji sprzętu i aplikacji informatycznych oraz usuwania awarii sprzętu, dokonuje informatyk lub firma na zlecenie Starostwa.

Tworzenie kopii awaryjnych.

1) Kopie awaryjne (zapasowe) należy wykonywać na nośnikach informatycznych przy pomocy programów standardowych, po każdej zmianie konfiguracji oprogramowania, np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, jednak nie rzadziej niż raz na kwartał.

2) Kopie awaryjne przechowuje się w miejscu uniemożliwiającym dostęp osób nieuprawnionych.

Identyfikacja użytkowników systemu informatycznego, służącego do przetwarzania danych osobowych.

§ 4

1. Dla każdego użytkownika systemu informatycznego, w którym przetwarza się informacje zawierające dane osobowe, Administrator bezpieczeństwa danych ustala odrębny identyfikator i hasło. Identyfikator wpisuje się do ewidencji i rejestruje w systemie informatycznym. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym powinien nastąpić po podaniu identyfikatora oraz właściwego hasła.
2. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie należy przydzielać go innej osobie.
3. Po otrzymaniu od administratora bezpieczeństwa haseł umożliwiających dostęp do konta użytkownik powinien niezwłocznie zmienić te hasła na inne, znane tylko sobie.

Hasła powinny spełniać następujące wymagania:

1) minimalna długość hasła powinna wynosić 6 znaków,
2) powinno zawierać duże oraz małe litery, cyfry i znaki specjalne,
3) nie należy używać wyrazów występujących we wszelkiego rodzaju słownikach, nawet jeśli zostaną uzupełnione innymi znakami, nie należy też używać żadnych wyrazów lub liczb występujących w danych osobowych użytkownika,
4) hasła nie wolno nigdzie zapisywać - ani na papierze, ani w postaci elektronicznej - **należy je zapamiętać.**
5) Zmiana haseł dla użytkowników następuje raz na miesiąc.
6) Nadzór nad zlecaniem dokonania czynności, o której mowa w ust. 3 należy do naczelnika wydziału, kierownika referatu w którym dokonuje się przetwarzania informacji zawierających dane osobowe.

Ewidencja osób zatrudnionych przy przetwarzaniu informacji zawierających dane osobowe.

§ 5

1. Ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych prowadzi pełnomocnik ds. ochrony danych osobowych.
2. Ewidencja powinna zawierać:
   1) imię i nazwisko osoby zatrudnionej przy przetwarzaniu danych osobowych,
   2) datę i numer kolejny udzielonego upoważnienia,
   3) identyfikator (mechanizm uwierzytelniania użytkownika),
   4) zakres funkcji środowiska komputerowego, z jakiego użytkownik faktycznie korzysta w przypadku pracy w sieci,
3) daty zmiany przydzielonego hasła.

§ 6

Każde domniemanie, przesłanka, fakt, wskazujący na naruszenie zasad ochrony danych osobowych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, w tym:

1. Stan urządzeń:
   - systemu zabezpieczeń obiektu,
   - aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,
2. Zawartość zbioru danych,
3. Ujawnione metody pracy,
4. Sposób działania programu,
5. Przebywanie osób nieupoważnionych wewnątrz obszaru przetwarzania danych osobowych,
6. Inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego, w tym obecność wirusów,

stanowi podstawę do natychmiastowego reagowania.

Sposób postępowania.

§ 7

1. O każdej sytuacji odbiegającej od normy, a w szczególności o przesłankach naruszenia zasad ochrony danych osobowych opisanych w § 6 należy:
   1) natychmiast poinformować administratora bezpieczeństwa informacji lub osobę przez niego upoważnioną,
   2) niezwłocznie sporządzić notatkę służbową z opisem zaistniałej sytuacji i przekazać ją administratorowi bezpieczeństwa informacji.
2. Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo zobowiązana jest do możliwie pełnego udokumentowania zdarzenia, celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.
3. Stwierdzone przez administratora informacji naruszenie zasad ochrony danych osobowych wymaga powiadomienia pełnomocnika ds. ochrony danych osobowych i administratora danych oraz natychmiastowej reakcji poprzez:
   1) usunięcie uchybień,
   2) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,
   3) wstrzymanie udostępnianie danych.

4. W sytuacji naruszenia zasad ochrony danych osobowych, po wcześniejszym wykonaniu czynności opisanych w ust. 3, administrator bezpieczeństwa informacji niezwłocznie sporządza informację na piśmie, przedstawiając administratorowi danych przyczyny, skutki i poczynione działania zabezpieczające i prewencyjne.

Postanowienia szczególne.

§ 8

1. Czynności polegające na przetwarzaniu informacji zawierających dane osobowe powinny być wykonywane w godzinach pracy Starostwa Powiatowego w Tarnobrzegu.

2. Wykonywanie czynności, o których mowa w ust. 1 poza godzinami pracy Starostwa wymaga zgody administratora danych lub pełnomocnika ds. ochrony danych osobowych.

§ 9

Naczelnicy wydziałów i kierownicy referatów oraz kierownicy jednostek organizacyjnych Powiatu są odpowiedzialni za sposób przetwarzania informacji, zawierających dane osobowe, ustalają częstotliwość wykonywania kopii awaryjnych, czasookres ich przechowywania oraz należyte zabezpieczenie przed dostępem osób postronnych jak również właściwy tryb postępowania w sytuacjach naruszania zasad ochrony danych osobowych.

§ 10

1. Pracownicy, zatrudnieni przy przetwarzaniu informacji zawierających dane osobowe, z wykorzystaniem sprzętu komputerowego zobowiązani są chronić wszelkie znane im lub będące w ich posiadaniu dane umożliwiające dostęp do zasobów środowiska informatycznego.
2. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów informatycznych w jego imieniu jest nielegalne, również za zgodą właściwego użytkownika. Nielegalne jest też korzystanie z plików lub innych zasobów innego użytkownika, nawet wtedy, gdy nie są one należycie chronione.

§ 11

Pracownicy, którzy dopuścili się do naruszenia bezpieczeństwa informacji zawierających dane osobowe, podlegają odpowiedzialności porządkowej lub dyscyplinarnej albo innej odpowiedzialności przewidzianej w przepisach prawa.