ZARZĄDZENIE Nr 138 / BOIN / 04

BURMISTRZA MIASTA CHEŁMŻY
Z DNIA 17 LISTOPADA 2004 ROKU

w sprawie ochrony danych osobowych w systemach informatycznych Urzędu Miasta Chełmży

Na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101 poz. 926, ze zm.) oraz § 6 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 roku, Nr 100, poz. 1024) **zarządza się, co następuje**:

§ 1. Zarządzenie określa podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 2. Ilekroć w zarządzeniu jest mowa o:

1) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1977 roku o ochronie danych osobowych zwaną dalej „ustawą";
2) identyfikatorze użytkownika – rozumie się przez to ciąg znaków cyfrowych stanowiących numer PESEL użytkownika jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym, tworzony przez Administratora Bezpieczeństwa Informacji Urzędu Miasta Chełmży i wprowadzany do systemu przez informatyka Urzędu;
4) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 roku – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, ze zm.);
5) sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 roku – Prawo telekomunikacyjne;
6) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
7) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nie autoryzowany;
9) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

10) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
11) uwierzytelnieniu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym:
1) podstawowy;
2) podwyższony;
3) wysoki.

§ 4. Poziom, co najmniej podstawowy stosuje się gdy:

1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz
2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

§ 5. Poziom, co najmniej podwyższony stosuje się, gdy:

1) w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz
2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

§ 6. Poziom wysoki stosuje się, gdy przynajmniej jedno z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

§ 7. System informatyczny służący do przetwarzania danych, który został dopuszczony przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, ze zm.) spełnia wymogi pod względem bezpieczeństwa na poziomie wysokim.

§ 8. Środki bezpieczeństwa na poziomie podstawowym:

1) Obszar, w którym przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2) Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych, jest dopuszczalne za zgodą administratora danych osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3) W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

4) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby: w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator, dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

5) System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed: działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej.
6) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
7) W przypadku, gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
8) Dane osobowe przetwarzane w systemie informatycznym zabezpiecz się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
9) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwa niezwłocznie po ustaniu ich użyteczności.
10) Osoby użytkujące komputer przenośny zawierający dane osobowe zachowują szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych. Do zabezpieczenia danych osobowych stosuje się ochronę kryptograficzną.
11) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe przeznaczone do:

    a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza w sposób uniemożliwiający ich odczytanie;
    b) przekazanie podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 9. Środki bezpieczeństwa na poziomie podwyższonym:

1) W przypadku, gdy do uwierzytelnienia użytkowników stosuje się hasło, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
2) Dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, przekazywane poza obszar przetwarzania danych osobowych, zabezpiecza się w sposób zapewniający poufność i integralność tych danych. Sposób zabezpieczenia poufności i integralności tych danych określa się w instrukcji zarządzania systemem informatycznym.
3) Stosuje się środki bezpieczeństwa określone w § 8 zarządzenia.

§ 10. Środki bezpieczeństwa na poziomie wysokim:

1) System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2) W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
3) Stosuje się środki ochrony kryptograficznej wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
4) Stosuje się środki bezpieczeństwa określone w § 8 i 9 zarządzenia.

§ 11. Traci moc zarządzenie Nr 14 / 99 Burmistrza Miasta Chełmży z dnia 30 listopada 1999 roku w sprawie ochrony danych osobowych i ich bezpieczeństwa w systemach informatycznych.

§ 12. Nadzór nad wykonaniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 13. Zarządzenie wchodzi w życie z dniem wydania.

BURMISTRZ MIASTA CHEŁMŻY

BURMISTRZ
mgr Jerzy Czerwiński

Otrzymują:

1) Wydział Organizacyjny, –
2) Wydział Finansowo – Księgowy, –
3) Wydział Gospodarki Miejskiej, –
4) Wydział Spraw Społecznych i Obywatelskich, –
5) Straż Miejska, –
6) Biuro Ochrony Informacji Niejawnych, –
7) Referat Gospodarczy, –
8) Kancelaria Tajna, –
9) Administrator Bezpieczeństwa Informacji – a / a. –

Chełmża, dnia 17. 11. 2004 r.

U Z A S A D N I E N I E

Nowelizacja ustawy o ochronie danych osobowych dokonana ustawą z dnia 22 stycznia 2004 roku o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 33, poz. 285) w art. 39 a zawiera delegację dla ministra do spraw administracji publicznej do określenia w porozumieniu z ministrem właściwym do spraw informatyzacji, w drodze rozporządzenia, sposobu prowadzenia i zakresu dokumentacji przetwarzania danych osobowych oraz podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z uwzględnieniem zapewnienia ochrony przetwarzanym danym osobowym odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępnienia danych osobowych i bezpieczeństwa przetwarzania danych. Rozporządzenie 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) określa katalog wymogów w zakresie systemów informatycznych przetwarzających dane osobowe i uchyla odpowiednie rozporządzenie w / w ministra z dnia 3 czerwca 1998 roku 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) stanowiące podstawę prawną Zarządzenia Nr 14 / 99 Burmistrza Miasta Chełmży z dnia 30 listopada 1999 roku w sprawie ochrony danych osobowych i ich bezpieczeństwa w systemach informatycznych. Mając na uwadze powyższe akty prawne przedstawiam do rozpatrzenia stosowny projekt zarządzenia.

Administrator Bezpieczeństwa Informacji

tkaczyk