

ZARZĄDZENIE Nr 107.2015
Burmistrza Olesna

z dnia 2 listopada 2015 r.

w sprawie wprowadzenia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie”

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) oraz § 3 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. z 2004 r. Nr 100, poz. 1024), **zarządza się, co następuje:**

§ 1.

Dla zapewnienia ochrony przetwarzania danych osobowych wprowadzam do stosowania „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie”, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Instrukcja, o której mowa w § 1 ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe w systemie informatycznym Urzędu Miejskiego w Oleśnie.

§ 3.

Nadzór nad realizacją postanowień zarządzenia powierzam Sekretarz Gminy Olesno.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr inż. Sylwester Lewicki

SEKRETARZ GMINY

Bożena Matusiak
dr Bożena Matusiak

Radca Prawny

Stawomir Skóra
mgr Stawomir Skóra

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie

§ 1.

1. Podstawą do opracowania i wdrożenia Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie, zwanej dalej „Instrukcją” jest:
 - 1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.);
 - 2) rozporządzenie 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).

§ 2.

Hełkroć w Instrukcji jest mowa o:

- 1) podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
- 2) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.);
- 3) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 4) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 5) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 z późn. zm.);
- 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 nieautoryzowany;
- 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) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3.

Za przestrzeganie w Urzędzie Miejskim w Oleśnie zapisów Instrukcji odpowiedzialny jest Administrator Danych lub wyznaczony Administrator Bezpieczeństwa Informacji.

§ 4.

W związku z tym, że w Urzędzie Miejskim w Oleśnie przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim, a w związku z tym wprowadza się poniższe postanowienia:

1. Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

- c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
 - d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
 - e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt a i b, 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.
 4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt d, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 6.

1. Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.
2. Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych i oraz przeglądów generalnych raz na rok.
3. W przypadku stwierdzenia usterek technicznych Administrator Bezpieczeństwa Informacji ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§ 7.

W przypadku stwierdzenia przez Administratora Bezpieczeństwa Informacji uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 8.

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz 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.