Zarządzenie Nr 102/2015
Wójta Gminy Radziejów
z dnia 31 grudnia 2015 r.
w sprawie wdrożenia Instrukcji zarządzania systemem informatycznym
w Urzędzie Gminy Radziejów

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jedn. Dz.U. z 2015 r., poz. 1515) oraz § 1 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),

zarządza się, co następuje:

§ 1. Wdraża się w Urzędzie Gminy Radziejów dokument o nazwie „Instrukcja zarządzania systemem informatycznym" w brzmieniu określonym w Załączniku nr 1 do niniejszego Zarządzenia.

§ 2. Zapisy „Instrukcji zarządzania systemem informatycznym" wchodzą w życie z mocą obowiązującą z dniem 1 stycznia 2016 r.

§ 3. Wykonanie zarządzenia powierza się Administratorowi Systemu Informatycznemu w Urzędzie Gminy Radziejów.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do Zarządzenia Nr 102/2015
Wójta Gminy Radziejów
z dnia 31 grudnia 2015 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY RADZIEJÓW

§ 1. Wyjaśnienie pojęć użytych w Instrukcji zarządzania systemem informatycznym, zwanej dalej Instrukcją.

Ilekroć w Instrukcji jest mowa o:

1) Urzędzie — rozumie się przez Urząd Gminy Radziejów;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2015 r., poz. 2135), zwaną dalej „ustawą";
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 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (tekst jedn. Dz. U. z 2014 r., poz. 243 z późn. zm.);
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy Prawo telekomunikacyjne;
7) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 2. Za przestrzeganie zapisów Instrukcji odpowiedzialny jest Administrator Systemu Informatycznego.

§ 3. W związku z tym, że w Urzędzie Gminy Radziejów są urządzenia systemu informatycznego, służącego do przetwarzania danych osobowych, połączone z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia ustala się stopień bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim.

§ 4. Obszar, w którym 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 osobowych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

§ 5. 1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła startowego jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachowywać je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. 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 oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

3. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może by
przydzielony innej osobie.

§ 6. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

a) poprzez zainstalowanie programu antywirusowego,

b) poprzez zainstalowanie firewall (zapora sieciowa),

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

§ 7. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w szafie pancernej w pomieszczeniu zamykanym na klucz oraz usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 8. Osoby użytkujące komputery przenośne zawierające dane osobowe zachowują szczególną ostrożność podczas transportu, przechowywania i użytkowania takiego sprzętu poza obszarem Urzędem, w szczególności stosują hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

§ 9. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 10. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) 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 pkt 1 i 2, 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 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 11. 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.

§ 12. Administrator Systemu Informatycznego ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w Urzędzie oraz dbać o dobry stan techniczny sprzętu. Zaleca się dokonywanie przeglądów okresowych co 90 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych Administrator Systemu Informatycznego ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych.

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

§ 14. 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.

Wójt Gminy

dr Marek Szuszman