ZARZĄDZENIE Nr 102/2015
WÓJTA GMINY DRZYCIM

z dnia 1 grudnia 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Drzycimiu oraz ustalenia zakresu jego obowiązków.

Na podstawie art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) w związku z art. 30 ust. 1 i art. 33 ust. 3 ustawy o samorządzie gminnym (Dz. U. z 2015 r. poz. 1515) zarządzam, co następuje:

§ 1. 1. Powołuję Pana Daniela Pożogę na funkcję Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Drzycimiu.

2. W przypadku nieobecności Administratora Bezpieczeństwa Informacji czynności wynikające z zakresu jego obowiązków wykonuje Administrator danych (Wójt) lub wskazany przez niego inny pracownik Urzędu Gminy.

§ 2. W zakresie czynności wynikających z pełnienia powierzonej funkcji i realizacji zadań związanych z ochroną danych osobowych Administrator Bezpieczeństwa Informacji podlega bezpośrednio Administratorowi danych.

§ 3. Do zakresu obowiązków Administratora Bezpieczeństwa Informacji należy:

1) opracowywanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz nadzorowanie przestrzegania zasad w niej określonych;
2) prowadzenie nadzoru nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz nad kontrolą przebywających w nich osób;
3) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
4) zabezpieczenie komputerów przenośnych hasłami dostępu przed nieautoryzowanym uruchomieniem oraz przed udostępnianiem osobom nieupoważnionym do przetwarzania danych;
5) prowadzenie ewidencji eksploatowanych komputerów przenośnych;
6) prowadzenie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
7) prowadzenie ewidencji dysków twardych;
8) zarządzanie hasłami użytkowników i nadzorowanie przestrzegania częstotliwości ich zmiany zgodnie z Polityką Bezpieczeństwa Informacji;
9) prowadzenie ewidencji nadawanych i odbieranych uprawnień;
10) nadawanie w imieniu Administratora danych upoważnień do przetwarzania danych osobowych;
11) prowadzenie ewidencji nadanych upoważnień do przetwarzania danych osobowych;
12) wykonywanie czynności związanych ze sprawdzaniem systemów informatycznych pod kątem obecności wirusów komputerowych oraz wykonywanie procedur uaktualniania systemów antywirusowych i ich konfiguracji;
13) Nadzorowanie wykonywania kopii awaryjnych oraz ich okresowe sprawdzanie pod kątem dalszej ich przydatności do odtwarzania danych w przypadku awarii systemu;
14) nadzorowanie systemów komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji;
15) nadzorowanie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemach informatycznych przetwarzających dane osobowe oraz kontrolowanie dostępu do danych osobowych poprzez:
    a) ustalenie identyfikatorów użytkowników i ich haseł (prowadzenie ewidencji osób

zatrudnionych przy przetwarzaniu danych osobowych),
b) dopilnowanie przestrzegania czasu zmiany haseł przez użytkowników,
c) dopilnowanie, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i hasła,
d) dopilnowanie, aby hasła użytkowników były objęte tajemnicą,
e) dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane, a ich hasła unieważnione;

16) nadzorowanie odpowiedniego ustawienia ekranów monitorów komputerowych;
17) udzielanie instruktaży i prowadzenie szkoleń ze wszystkimi osobami nowo zatrudnianymi w Urzędzie;
18) przyjmowanie od osób nowo zatrudnionych oświadczeń o zachowaniu danych w tajemnicy i o zapoznaniu się z obowiązującymi w Urzędzie przepisami dotyczącymi ochrony danych osobowych i bezpieczeństwa teleinformatycznego;
19) prowadzenie szkoleń z pracownikami Urzędu z zakresu ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego;
20) wspomaganie pracowników w czynnościach związanych z rejestracją zbiorów danych osobowych i zgłaszaniem zmian w zarejestrowanych już zbiorach danych oraz związanych z rejestracją zbiorów danych osobowych zawierających „wrażliwe" dane osobowe;
21) prowadzenie korespondencji z Biurem Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w sprawach związanych z ochroną danych osobowych;
22) nadzorowanie umów dotyczących udostępniania lub powierzania przetwarzania danych osobom lub podmiotom zewnętrznym w zakresie stosowania zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych;
23) podejmowanie działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu jego zabezpieczeń lub informacji o zmianach w sposobie działania programu i urządzeń, wskazujących na naruszenie bezpieczeństwa danych;
24) w sytuacji wystąpienia naruszenia bezpieczeństwa danych, prowadzenie analizy okoliczności i przyczyn, które do tego doprowadziły, a także przygotowywanie i przedstawianie Administratorowi danych propozycji wprowadzenia odpowiednich zmian do Polityki Bezpieczeństwa Informacji, mających na celu wyeliminowanie lub ograniczenie wystąpienia podobnych sytuacji w przyszłości;
25) prowadzenie i publikowanie jawnego rejestru zbiorów danych osobowych przetwarzanych przez Administratora danych;
26) przeprowadzanie sprawdzeń oraz przygotowywanie stosownych sprawozdań na wniosek GIODO;
27) inne obowiązki przewidziane w ustawie o ochronie danych osobowych, a nie wymienionych w niniejszym zarządzeniu.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy
mgr Waldemar Moczyński