Z A R A Ą D Z E N I E Nr 86/2015

WÓJTA GMINY TUROŚŃ KOŚCIELNA

z dnia 31 grudnia 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Turośń Kościelna

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2015 r. poz. 1515) i art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 poz. 1182 z późn. zm.) zarządzam, co następuje:

§ 1. Z dniem 2 stycznia 2016 r. powołuje Pana Marka Grądzkiego na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Turośń Kościelna.

§ 2. Do zakresu obowiązków Administratora Bezpieczeństwa Informacji należą:

1) Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b) nadzorowanie opracowania i analizowanie dokumentacji, o której mowa w art. 36 ust.2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2) Prowadzenie rejestru zbioru danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa a art. 43 ust. 1 , zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182 z późn. zm.).
3) Prowadzenie nadzoru nad fizycznym zabezpieczeniem pomieszczeń , w których przetwarzane są dane osobowe.
4) Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
5) Przestrzeganie, aby komputery przenośne w których przetwarzane są dane osobowe, zabezpieczone były hasłami dostępu przed nieautoryzowanym uruchomieniem oraz przed udostępnianiem osobom nieupoważnionym do przetwarzania danych osobowych. Osoby posiadające komputery przenośne z zapisanymi w nich danymi osobowymi nie mają prawa wynosić ich poza obszar budynku Urzędy Gminy Turośń Kościelna.
6) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których są zapisane dane osobowe. Dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji należy pozbawić zapisu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności Administratora Bezpieczeństwa Informacji, a w przypadku nieobecności

Administratora Bezpieczeństwa Informacji, osoby upoważnionej przez Administratora Bezpieczeństwa Informacji.

7) Zarządzanie hasłami użytkowników i nadzorowanie przestrzegania procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które zawarte są w Polityce Bezpieczeństwa Informacji.
8) Nadzorowanie czynności związanych ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.
9) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.
10) Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny.
11) Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych. Nadzorowanie powinno obejmować:
    a) ustalenie identyfikatorów użytkowników haseł,
    b) dopilnowanie, aby hasła użytkowników były zmieniane nie rzadziej niż raz w miesiącu,
    c) dopilnowanie, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
    d) dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane, a ich hasła unieważnione,
12) Przestrzeganie, aby jeżeli istnieją odpowiednie możliwości techniczne, ekrany ,monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie się wyłączały po upływie ustalonego czasu nieaktywności użytkownika.
13) Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa powyżej powinny mieć na celu wykrycie przyczyn lub sprawcy zaistniałej sytuacji i jej usuniecie.
14) Analizowanie sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeżeli takie nastąpiło) i przygotowanie oraz przedstawienie Administratorowi Danych Osobowych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych. Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości.
15) Przeszkolenie osób przetwarzających dane osobowe w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych.
16) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr Grzegorz Jakuć