Zarządzenie Nr SEG/8/2016
WÓJTA GMINY ŚWIDWIN
z dnia 10 lutego 2016r.

w sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Świdwinie

Na podstawie art. 31 i art. 33 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2015r., poz. 1515 ze zm.) w związku z art. 36a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r., poz. 2135) zarządzam, co następuje:

§ 1. Powołuje się Pana **Jarosława Miedzika** na stanowisko Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy w Świdwinie, na zasadzie outsourcingu usług.

§ 2. Ustala się ramowy zakres zadań ABI w Urzędzie Gminy w Świdwinie, zgodnie z załącznikiem do niniejszego zarządzenia.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Świdwin.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY ŚWIDWIN

WÓJT
mgr Kazimierz Lechocki

Załącznik
do Zarządzenia Nr SEG/8/2016
Wójta Gminy Świdwin
z dnia 10 lutego 2016r.

Zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji
W Urzędzie Gminy w Świdwinie

I. Administrator Bezpieczeństwa Informacji – zwany dalej ABI wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnienia nadanego przez Administratora Danych Osobowych.

II. Zadaniem ABI jest realizacja przedsięwzięć określonych w art. 36a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r., poz.2135) oraz w zarządzeniach Administratora Danych Osobowych, a w szczególności:

1) Zapewnienie przestrzegania przepisów o ochronie danych osobowych, 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 aktualizacja dokumentacji, o której mowa w art. 36 ust.2 ustawy o ochronie danych osobowych oraz przestrzegania zasad w niej określonych,
   c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2) Prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust.1 ustawy o ochronie danych osobowych, zgodnie z wymogami ustawy.
3) Zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
4) Prowadzenie ewidencji osób upoważnionych do ich przetwarzania, zgodnie z wymogami ustawy.
5) Zgłaszanie zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust.1 i 1a ustawy.
6) Stosowanie środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednich do zagrożeń oraz kategorii danych.
7) Zabezpieczenie danych osobowych przed udostępnianiem osobom nieupoważnionym lub zabraniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem.
8) Nadzór nad stosowaniem przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania.
9) Analiza stanu ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń.
10) Realizacja zadań w zakresie:
   a) rozpatrywania skarg i wniosków dotyczących przetwarzania i ochrony danych,
   b) tworzenia projektów zarządzeń, instrukcji i wytycznych Administratora,
   c) przygotowanie informacji w zakresie rejestracji zbiorów w GIODO lub zmian w przetwarzaniu danych,
   d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych,
   e) odnotowania i dokumentowania zmian w lokalizacji obszarów przetwarzania danych.

III. ABI realizując swoje zadania współpracuje z Administratorem Systemu Informatycznego (ASI).

IV. Wykonując swoje czynności ABI działa w imieniu Administratora Danych Osobowych i posiada uprawnienia do:

1) wskazywania zastosowania odpowiednich zabezpieczeń i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych,
2) wnioskowanie o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych,
3) udzielanie wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa,
4) zbieranie od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych

WÓJT
mgr Kazimierz Lechocki