ZARZĄDZENIE 473/2015

Wójta Gminy Pątnów

z dnia 22 czerwca 2015 r.

W sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Pątnów.

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. 2013 r., poz. 594, zm. poz. 645 i 1318 oraz z 2014 r. poz. 379 i 1072) art. 36a ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2014 r., poz. 1182, zm. poz. 1662.), zarządzam, co następuje:

§ 1.

1. Wyznaczam Pana Mateusza Drab na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Pątnów.
2. Zakres działania Administratora Bezpieczeństwa Informacji stanowi załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
dr Jacek Olczyk

Załącznik do Zarządzenia Nr 473/2015

Wójta Gminy Pątnów

z dnia 22 czerwca 2015 r.

Zakres zadań oraz uprawnień i upoważnienia administratora bezpieczeństwa informacji w Urzędzie Gminy Pątnów

I. Administrator bezpieczeństwa informacji - zwany dalej ABI wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnień i pełnomocnictw nadanych przez Administratora Danych Osobowych.

II. Celem działania ABI jest nadzorowanie i kontrolowanie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w komórkach organizacyjnych Urzędu Gminy Pątnów.

III. Zadaniem ABI jest realizacja przedsięwzięć określonych w art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz.U. z 2014 r. poz1182 z późn. zm.) oraz zarządzeniach Administratora Danych Osobowych, a w szczególności nadzorowanie, kontrolowanie i koordynowanie:

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 aktualizowania dokumentacji, o której mowa w art. 36 ust.2 oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych poprzez bieżące doradztwo oraz przeprowadzanie przynajmniej raz w roku szkolenia w tym zakresie;
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, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i la 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) realizowanie zadań w zakresie:

a) rozpatrywania skarg i wniosków dotyczących przetwarzania i ochrony danych;
b) tworzenia projektów zarządzeń, instrukcji i wytycznych Administratora;
c) przygotowywania informacji w zakresie rejestracji zbiorów w GIODO lub zmian w zakresie przetwarzania danych;
d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych;
e) odnotowywania i dokumentowania zmian w lokalizacji obszarów przetwarzania danych.

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

1) Wskazywania zastosowania odpowiednich zabezpieczeń technicznych 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 okoliczności powstania zagrożeń dla bezpieczeństwa i ochrony danych osobowych;
5) szkolenie pracowników z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji;
6) kontrolowanie pracowników poprzez audyty związane z bezpieczeństwem informacji oraz ochroną danych osobowych.

WÓJT
dr Jacek Olczyk