Zarządzenie Nr 473/18
Burmistrza Śmigla
z dnia 24 maja 2018 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji.

Na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U.2016 poz. 922) zarządzam, co następuje:

§ 1

Z dniem 24 maja 2018 r. powołuję Pana Jarosława Bartkowiaka do pełnienia funkcji Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim Śmigla.

§ 2

Zakres uprawnień i obowiązków Administratora Bezpieczeństwa Informacji określa załącznik nr 1 do niniejszego zarządzenia.

§ 3

Wykonanie zarządzenia powierza się Sekretarzowi Śmigla.

§ 4

Traci moc Zarządzenie Nr 257/16 Burmistrza Śmigla z dnia 4 października 2016 r.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Śmigla

/-/ Małgorzata Adamczak

Załącznik nr 1
do Zarządzenia Nr 473/18
Burmistrza Śmigla
z dnia 24 maja 2018 r.

Ramowy zakres uprawnień i obowiązków Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim Śmigla

1. Administrator Bezpieczeństwa Informacji, zwany dalej ABI wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnienia nadanego przez Administratora Danych Osobowych.
2. Do zadań ABI, zgodnie z art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U.2016 poz. 922), zwanej dalej ustawą, należy:
   1) zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
      a) sprawdzenie zgodności przetwarzania danych osobowych z przepisami ustawy oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
      b) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz przestrzegania zasad określonych w ustawie,
      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, zgodnie z jej wymogami;
   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 1 a 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) nadzorowanie stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania;
   9) analizowanie 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 Danych;
      c) przygotowywania 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) odnotowywania i dokumentowania zmian w lokalizacji obszarów przetwarzania danych.
3. ABI realizując swoje zadania współpracuje z Administratorem Systemu Informatycznego (ASI).
4. 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 ograniczeniu zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych;
   3) udzielenie wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa;
   4) zbieranie od użytkowników, ich przełożonych pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.