

Zarządzenie Nr 257/16
Burmistrza Śmigła
z dnia 4 października 2016r.

w sprawie: powołania Administratora Bezpieczeństwa Informacji.

Na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U.2016.922 z dnia 28.06.2016) zarządzam, co następuje:

§ 1

Z dniem 4 października 2016 r. powołuję Panią Sylwię Nowicką do pełnienia funkcji Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim Śmigła.

§ 2

W zakresie wykonywanych zadań i pełnionych obowiązków Administrator Bezpieczeństwa Informacji podlega bezpośrednio Burmistrzowi Śmigła.

§ 3

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

§ 4

Wykonanie Zarządzenia powierza się Zastępcy Burmistrza.

§ 5

Traci moc Zarządzenie Nr 137/16 Burmistrza Śmigła z dnia 4 stycznia 2016r.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Śmigła

/-/ Małgorzata Adamczak

*Załącznik nr 1
do Zarządzenia Nr 257/16
Burmistrza Śmigła
z dnia 4 października 2016r.*

Ramowy zakres uprawnień i obowiązków Administradora Bezpieczeństwa Informacji w Urzędzie Miejskim w Śmiglu

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 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2014r. poz.1182, z późn. zm.) zwanej dalej ustawą, należy:
 - 1) zapewnieniu przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
 - a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o 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) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
 - 2) prowadzeniu 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) zapewnieniu kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
 - 4) prowadzeniu ewidencji osób upoważnionych do ich przetwarzania, zgodnie z wymogami ustawy;
 - 5) zgłaszaniu zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy;
 - 6) stosowaniu środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednich do zagrożeń oraz kategorii danych;
 - 7) zabezpieczeniu danych osobowych przed udostępnianiem osobom nieupoważnionym lub zabranieniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem;

- 8) nadzorowaniu stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania;
- 9) analizowaniu stanu ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń;
- 10) realizowaniu 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 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 osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.