BURMISTRZ MIASTA
KĘTRZYN
Krzysztof Hećman

Zarządzenie Nr 6/2016
Burmistrza Miasta Kętrzyn
z dnia 15 stycznia 2016 r.

o zmianie Zarządzenia Nr 45/13 Burmistrza Miasta Kętrzyn z dnia 4 lutego 2013 r. w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miasta Kętrzyn.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. 2015 r., poz. 1515), art. 36 a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. 2015 r., poz. 2135) oraz Zarządzenia Nr 270/12 Burmistrza Miasta Kętrzyn z dnia 17 grudnia 2012 r. w sprawie wprowadzenia w życie „ Polityki bezpieczeństwa danych osobowych w Urzędzie Miasta Kętrzyn" oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Kętrzyn", zmienionego Zarządzeniem Nr 8/13 Burmistrza Miasta Kętrzyn z dnia 10 stycznia 2013 r. zarządzam, co następuje:

§ 1

W Zarządzeniu Nr 45/13 Burmistrza Miasta Kętrzyn z dnia 4 lutego 2013 r. w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miasta Kętrzyn § 1 otrzymuje brzmienie:
„ § 1. 1. Powołuję Pana Tadeusza Sienkiela na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Miasta Kętrzyn.
2. Zakres działania Administratora Bezpieczeństwa Informacji (ABI) stanowi załącznik do niniejszego zarządzenia".

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Sporządziła: J. Łastówka

BURMISTRZ MIASTA
KĘTRZYN
Krzysztof Hećman

Załącznik do Zarządzenia
Nr 6/2016 Burmistrza Miasta
Kętrzyn z dnia 15 stycznia 2016 r.

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych w imieniu i na rzecz Administratora Danych Osobowych.

Do zadań Administratora Bezpieczeństwa Informacji należy:

1. Prowadzenie oraz aktualizacja dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, określonych w „Polityce bezpieczeństwa danych osobowych" i w „ Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych",
2. Nadzorowanie przestrzegania zasad określonych w „Polityce bezpieczeństwa danych osobowych" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych",
3. Szkolenie osób dopuszczonych do przetwarzania danych osobowych lub przebywania w obszarze przetwarzania danych osobowych z zakresu zasad przetwarzania i ochrony tych danych oraz zasad bezpieczeństwa informatycznego w oparciu o przygotowanie przez siebie materiały szkoleniowe oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. potwierdzenie przeszkolenia),
4. Nadzorowanie prawidłowości udostępniania danych osobowych odbiorcom danych,
5. Nadzorowanie zamieszczania w umowach z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami, którym powierzono przetwarzanie danych osobowych lub konserwację urządzeń służących do przetwarzania danych oraz pracownikami tych firm, a także w innych dokumentach odpowiednich zapisów dotyczących ochrony danych osobowych,
6. Nadzorowanie wdrożenia adekwatnych do zagrożeń środków fizycznych, a także organizacyjnych i technicznych służących zapewnieniu bezpieczeństwa ,
7. Nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe w zakresie związanych z bezpieczeństwem tych danych osobowych,
8. Koordynowanie kontroli wewnętrznych z zakresu przestrzegania przepisów o ochronie danych osobowych, w tym prowadzenie szczegółowej dokumentacji z kontroli dot.:
a. zakresu przestrzegania przepisów o ochronie danych osobowych,
b. stwierdzonych naruszeń bezpieczeństwa danych osobowych, obejmujących m.in. analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło).
9. Podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia bezpieczeństwa systemu informatycznego oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. opis incydentu, osoby biorące udział, dokumentacja dot. reakcji na incydent).