BURMISTRZ
Szczawna - Zdroju

ZARZĄDZENIE NR 33/2013
BURMISTRZA SZCZAWNA ZDROJU
z dnia 29 kwietnia 2013 r.

w sprawie powołania ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI w Urzędzie Miejskim w Szczawnie-Zdroju.

Na podstawie art. 33 ust. 4 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (jt. Dz.U. z 2001 r. Nr 142, poz. 1591 ze zm.), w związku z art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (jt. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.),

§ 1.

1. Wyznaczam Panią **TERESĘ BEBEL** – Sekretarza Miasta Szczawna-Zdroju do pełnienia funkcji **ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI** w Urzędzie Miejskim w Szczawnie-Zdroju.
2. Zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji określono w załączniku do zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Szczawna-Zdroju
Tadeusz Wlaźlak

ADWOKAT
Marek Żegnałek

Załącznik do Zarządzenia Nr 33/2013
Burmistrza Szczawna-Zdroju
z dnia 29 kwietnia 2013 r.

Zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Szczawnie-Zdroju

1. Zapewnienie ochrony i bezpieczeństwa danych osobowych zawartych z zbiorach systemów informatycznych Urzędu.
2. Kontrolowanie prawidłowego wykorzystania wdrożonych do stosowania dokumentów wewnętrznych.
3. Analizowanie aktualności dokumentów wewnętrznych i składanie wniosków do Administratora Danych - Burmistrza o zmianę ich treści.
4. Kontrolowanie pracowników i innych osób upoważnionych pod względem wykonywania przez nich obowiązków związanych z ochroną przetwarzanych danych osobowych.
5. Kontrolowanie służb informatycznych pod względem skuteczności zastosowanych środków fizycznych, sprzętowych i programowych mających na celu zachowanie poufności, integralności i rozliczalności danych osobowych, w tym:
   a) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
   b) Nadzór nad zarządzaniem hasłami użytkowników przetwarzających dane osobowe.
   c) Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
   d) Nadzór nad przeglądami, konserwacją oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi czynnościami wykonywanymi na bazach danych osobowych.
6. Kontrolowanie służb zajmujących się przechowywaniem i archiwizacją dokumentów papierowych zawierających dane osobowe, pod względem prawidłowego zabezpieczenia tych dokumentów.
7. Kontrolowanie podmiotów trzecich, którym powierzono do przetwarzania dane osobowe, pod względem zabezpieczenia tych danych.
8. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. Kontrolowanie fizycznego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.
10. Udział w czynnościach kontrolnych dokonywanych przez uprawnione w zakresie ochrony danych osobowych organy państwowe.
11. Weryfikowanie sprzętu i oprogramowania eksploatowanego przez Administratora Danych pod względem zgodności z przepisami o ochronie danych osobowych.
12. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

13. Podejmowanie działań w przypadku naruszeń ochrony danych osobowych, w tym przywrócenie stanu prawidłowego, zidentyfikowanie przyczyn naruszenia i osób odpowiedzialnych, przedstawienie wniosków Administratorowi Danych.
14. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia bezpieczeństwa ochrony danych osobowych.
15. Nadzór i kontrola nad przestrzeganiem POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH w Uzdrowiskowej Gminie Miejskiej Szczawno-Zdrój.

W przypadku stwierdzenia nieprawidłowości w zakresie zabezpieczenia danych osobowych Administrator Bezpieczeństwa Informacji ma obowiązek:

1. Pouczać i instruować osoby, które dopuściły się uchybień, a także raportować o błędach Administratorowi Danych mając na celu przywrócenie stanu zgodnego z prawem.
2. Zwracać się do Administratora Danych o dokonanie zmian w zakresie stosowanych zabezpieczeń organizacyjnych i technicznych.
3. Przedstawiać Administratorowi Danych raporty dotyczące stanu zabezpieczenia danych osobowych, w tym propozycje poprawiające bezpieczeństwo danych oraz wnioski dotyczące odpowiedzialności osób winnych uchybień.