Załącznik
do Zarządzenia Nr 14/2015
Starosty Szydłowieckiego

Zakres zadań Administratora Bezpieczeństwa Informacji (ABI)

Do zadań Administratora Bezpieczeństwa Informacji należy:

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 ustawy o ochronie danych osobowych, oraz przestrzegania zasad w niej określonych,
   c) zapewnianie 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 o ochronie danych osobowych, zgodnie z wymogami ustawy.
3. Prowadzenie ewidencji osób upoważnionych do ich przetwarzania, zgodnie z wymogami ustawy.
4. Zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
5. Zgłaszanie zbiorów danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a 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. Wskazywania zastosowania odpowiednich zabezpieczeń technicznych i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych.
10. Wnioskowanie o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych.
11. Udzielanie wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa.
12. Zbieranie od użytkowników, ich przełożonych pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.