Zakład
Gospodarki Komunalnej i Mieszkaniowej
62-060 Stęszew, ul. Mosińska 15
Tel. 61 8134-182

Zarządzenie Nr 3/2015

Dyrektora Zakładu Gospodarki Komunalnej i Mieszkaniowej w Stęszewie

z dnia 02.03.2015 r

w sprawie wprowadzenia Polityki Bezpieczeństwa przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym oraz powołania Administratora Bezpieczeństwa Informacji

Na podstawie art. 36 i 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisu § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zarządzam co następuje:

§1

1. Dla zapewnienia bezpieczeństwa informacji i ochrony przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Stęszewie wprowadzam do stosowania:
   1) Politykę bezpieczeństwa przetwarzania danych osobowych, zwaną dalej Polityką Bezpieczeństwa, stanowiącą załącznik nr 1 do niniejszego zarządzenia,
   2) Instrukcję zarządzania systemem informatycznym, stanowiącą załącznik nr 2 do niniejszego zarządzenia.
2. Polityka Bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Zakładu Gospodarki Komunalnej i Mieszkaniowej w Stęszewie.
3. Z treścią dokumentów, o których mowa w §1 obowiązek zapoznania się mają wszyscy pracownicy Zakładu Gospodarki Komunalnej i Mieszkaniowej w Stęszewie oraz osoby przetwarzające dane osobowe w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Stęszewie na podstawie zawartej umowy, dotyczącej świadczenia na rzecz Zakładu usług informatycznych.

§2

1. W celu zapewnienia przestrzegania zasad bezpieczeństwa informacji i ochrony przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Stęszewie (dalej Zakład), powołuję Panią Beatę Baranowską (Zastępcę Głównego Księgowego) do pełnienia funkcji Administratora Bezpieczeństwa Informacji.
2. W zakresie zadań wykonywanych jako Administrator Bezpieczeństwa Informacji, Pani Beata Baranowska podlega bezpośrednio Administratorowi Danych Osobowych w Zakładzie - Dyrektorowi Zakładu Gospodarki Komunalnej i Mieszkaniowej w Stęszewie i przed nim odpowiada za prawidłowe i terminowe wykonywanie zadań wymienionych w § 3 niniejszego zarządzenia.
3. Administrator Bezpieczeństwa Informacji zobowiązany jest do znajomości niezbędnych przepisów prawa oraz procedur wewnętrznych, obowiązujących w Zakładzie, ścisłego ich przestrzegania oraz posiadania wiedzy do wykonania pracy na zajmowanym stanowisku.
4. Do zadań Administratora Bezpieczeństwa Informacji należy:
   1) Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych Osobowych;
   2) Nadzorowanie opracowania i aktualizowania dokumentacji wewnętrznej związanej z ochroną danych osobowych w jednostce oraz przestrzegania zasad w niej określonych,
   3) Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   4) Prowadzenie rejestru zbiorów danych osobowych przetwarzanych w Zakładzie z uwzględnieniem wyłączeń z mocy ustawy;
   5) Zapewnienie zgodności wykonywania czynności przetwarzania danych zgodnie z uregulowaniami obowiązującej w Polityce Bezpieczeństwa;
   6) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
   7) Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;
   8) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony przetwarzanych danych osobowych w Zakładzie;
   9) Kontrola przestrzegania zasad ochrony – systematyczne, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

10) Sporządzanie sprawozdania z przeprowadzonej kontroli wewnętrznej oraz przedkładanie sprawozdania do wiadomości Administratora Danych Osobowych;
11) Przegląd i aktualizacja procedur wewnętrznych zawartych w dokumencie „Polityka bezpieczeństwa" oraz w „Instrukcji zarządzania systemem informatycznym" – przynajmniej raz w roku do dnia 15 lutego każdego roku;
12) Aktualizacja zapisów w:
    a) „Wykazie budynków i pomieszczeń tworzących obszar, w którym przetwarzane
    są dane osobowe".
    b) „Wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych".
13) Bieżące prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w Zakładzie;
14) Przegląd i aktualizacji stosowanych w Zakładzie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
15) Przeprowadzanie szkoleń wstępnych oraz okresowych z zakresu przetwarzania danych osobowych dla pracowników Zakładu;
16) Gromadzenie złożonych przez pracowników Zakładu oświadczeń o wyrażeniu zgody
    na przetwarzanie danych osobowych;
17) Uzgadniania z Administratorem Danych wszelkich wydatków związanych z niezbędnymi naprawami i dokonuje drobnych zakupów potrzebnych do konserwacji sieci komputerowej w pomieszczeniach Zakładu.

5. Upoważniam Administratora Bezpieczeństwa Informacji do:
    1) wejścia i kontroli pomieszczeń w których przetwarzane są dane osobowe, w szczególności prawo wejścia i kontroli stanu zabezpieczenia archiwum oraz pomieszczenia serwerowni;
    2) wykonywania kontroli wewnętrznej w Zakładzie, polegającej na sprawdzeniu zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontroli pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
    3) prowadzenia postępowań wyjaśniających w przypadkach podejrzenia naruszenia bezpieczeństwa informacji,

4) wnioskowania o upoważnienie pracownika do przetwarzania danych osobowych lub o zmianę zakresu upoważnienia pracownika do przetwarzania danych osobowych;
5) zgłaszania wniosków i propozycji dotyczących usprawnienia pracy i polepszenia jej organizacji.

§3

Zarządzenie wchodzi w życie z dniem podpisania

Dyrektor
Zbigniew Grzesikowiak
2.03.2015