ZARZĄDZENIE NR 120/20/2014

Wójta Gminy Bojszowy

z dnia 26.05.2014 r.

w sprawie: powołania Administratora Bezpieczeństwa Informacji

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zm.*) oraz zgodnie z wymogami § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. Nr 100 poz. 1024*), zwanego dalej rozporządzeniem zarządza się, co następuje:

§ I

Wyznacza się Pana Grzegorza Skipioł na Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Bojszowy.

§ 2

Ustala się zakres zadań Administratora bezpieczeństwa informacji w brzmieniu załącznika nr 1 do zarządzenia.

§ 3

Zmienia się Zarządzenie Nr 0152/61/2009 w sprawie: Polityki bezpieczeństwa ochrony danych osobowych i instrukcji zarządzania systemami służącymi do przetwarzania danych osobowych poprzez wykreślenie pkt 4 i 5.

§ 4

Wykonanie zarządzenia powierza się Sekretarzowi Gminy

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do zarządzenia Nr 120/20/2014
z dnia 26.05.2014 r.

Do obowiązków Administratora Bezpieczeństwa Informacji należy w szczególności:

1. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych w tym opracowanie i aktualizowanie dokumentacji przetwarzania danych (polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącymi do przetwarzania danych osobowych).
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i instrukcji zarządzania systemami służącymi do przetwarzania danych osobowych.
3. Nadzór nad wdrożeniem dokumentacji przetwarzania danych.
4. Nadzór nad rejestracją zbiorów danych osobowych oraz wszelkimi zmianami z nimi związanymi. Inicjowanie działań związanych z koniecznością zgłoszenia zbioru do GIODO.
5. Prowadzenie "Ewidencji osób upoważnionych do przetwarzania danych osobowych".
6. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
7. Nadzór mad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
8. Kontrola działań Pracowników Urzędu Gminy pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
9. Inicjowanie i podejmowanie przedsięwzięć w zakresie poprawy zabezpieczeń ochrony danych osobowych w Urzędzie Gminy.
10. Tworzenie i weryfikacja procedur przetwarzania danych.
11. Sprawdzanie formularzy służących do zbierania danych osobowych pod kątem ich zgodności z przepisami o ochronie danych osobowych.
12. Okresowe przeprowadzanie kontroli (audytu) przetwarzania danych i przedstawianie pracodawcy stosownych wniosków.
13. Weryfikowanie systemu informatycznego pod kątem wymagań przepisów o ochronie danych osobowych i zgłaszanie pracodawcy stosownych wniosków w tym zakresie.
14. Nadzór nad prawidłowym przechowywaniem i udostępnianiem dokumentacji zawierającej dane osobowe.
15. Reagowanie na sytuacje naruszenia bezpieczeństwa danych i raportowanie na ten temat do Administratora Danych Osobowych. Prowadzenie postępowania wyjaśniającego w tym zakresie.
16. Kontrola zawartości strony internetowej pod kątem ewentualnego przetwarzania danych osobowych.
17. Prowadzenie okresowych szkoleń dla pracowników w zakresie ochrony danych osobowych.
18. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji

19. Zarządzanie kontami użytkowników (ustalenie identyfikatorów i haseł, ich przyznawanie, anulowanie, resetowanie i ochrona). Dbałość o właściwe ustawienie urządzeń, tak, aby minimalizować możliwość wycieków informacji
20. Inicjowanie przeprowadzania symulowanego włamania do systemu i ustalanie aktualnego poziomu zabezpieczeń. Wnioskowanie do Wójta o środki na rozbudowę zabezpieczeń systemu ochrony danych osobowych.
21. Nadzór nad aktualizacją i konfiguracją oprogramowania antywirusowego oraz systemowego. Okresowe sprawdzanie systemu pod kątem obecności wirusów, koni trojańskich i innych zagrożeń komputerowych.
22. W ramach monitoringu wynikającego z Instrukcji zarządzania systemami służącymi do przetwarzania danych osobowych przeprowadzanie następujących działań:
    a. okresowe sprawdzanie kopii zapasowych pod względem przydatności do odtworzenia danych;
    b. kontrola ewidencji nośników środków magnetycznych i optycznych;
    c. sprawdzanie częstotliwości zmian haseł;
    d. kontrola wysyłanych i odbieranych danych w systemach teleinformatycznych;
23. Przeprowadzanie kontroli w zakresie stosowania przepisów ustawy o ochronie danych osobowych, w tym przestrzegania zasad bezpieczeństwa osobowego i instrukcji zarządzania systemami służącymi do przetwarzania danych na wniosek Administratora Danych.