Zarządzenie nr SG.0050.15.2013
Wójta Gminy Ślemień z dnia 28 lutego 2013 roku
w sprawie organizacji przetwarzania danych
osobowych przez pracowników Urzędu Gminy w Ślemieniu.

Na podstawie art.30 ust.1 ustawy z dnia 8 marca 1990 r. 0 samorządzie gminnym (Dz.U. z 2001r., nr 142, poz.159l z późn. zm.) oraz art. 7 pkt.4, art.26 ust.1 oraz art.36 do art. 39 i art.40 ustawy o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002r., nr 10l, poz.926 z późn. zm.) zarządza się, co następuje:

§1

Zarządzenie określa:

1. zasady zgłaszania do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO)zbiorów danych oraz wydawania pracownikom Urzędu Gminy w Ślemieniu upoważnień do przetwarzania danych osobowych
2. powołanie administratora bezpieczeństwa informacji oraz określenie jego obowiązków;
3. obowiązki osób funkcyjnych i uprawnionych pracowników Urzędu Gminy (UG) do przetwarzania danych osobowych i ich ochrony.

§2

Ilekroć w zarządzeniu jest mowa o:

1. ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, zwaną dalej „ustawą",
2. rozporządzeniu - rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004r., nr 100, poz. 1024), zwanego dalej „rozporządzeniem".

§3

Na administratora bezpieczeństwa informacji wyznaczam Pana Romana Wajdzika, którego czynię odpowiedzialnym za:

1. nadzorowanie w UG przestrzegania zasad ochrony przetwarzanych danych osobowych oraz zaleceń zawartych w „Polityce bezpieczeństwa" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";
2. utrzymanie w ciągłej aktualizacji „Polityki bezpieczeństwa" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";
3. dostosowanie właściwych poziomów bezpieczeństwa o których mowa w § 6 „rozporządzenia" do kategorii przetwarzanych danych oraz zagrożeń związanych z przetwarzaniem danych w systemie informatycznym;
4. nadzorowanie bieżącego usuwania przez użytkowników z systemów informatycznych danych osobowych przetwarzanych wyłącznie w celu edycji tekstu;
5. monitorowanie wdrożonych zabezpieczeń systemu informatycznego;
6. stosowanie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej;
7. ustalanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu, w przypadku jeżeli dostęp do systemu informatycznego posiada więcej niż jedna osoba;
8. sprawdzanie czy pracownicy upoważnieni do przetwarzania danych osobowych w systemach informatycznych dokonują zmiany haseł uwierzytelniających nie rzadziej niż co 30 dni;
9. dostosowanie systemów informatycznych służących do przetwarzania danych osobowych do wymogów § 7 „rozporządzenia" oraz załącznika do niego wydanego;

10. w przypadku stwierdzenia przetwarzania danych osobowych niezgodnie z przepisami prawa, niezwłoczne podjęcie działania zmierzającego do wyeliminowania zaistniałej sytuacji, a następnie zawiadomienie administratora danych osobowych o zaistniałym zdarzeniu;
11. niedopuszczenie do przetwarzania danych przez osoby do tego nieuprawnione;
12. nadzorowanie wykonywania kopii zapasowych zbiorów danych, a także ich przechowywania wyłącznie w miejscach zabezpieczających przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
13. nadzorowanie aby uszkodzone urządzenia, dyski lub inne elektroniczne nośniki informacji przed oddaniem do naprawy były pozbawione zapisu danych osobowych, a w przypadku ich likwidacji , w obecności komisji powołanej przez wójta powinny zostać na tyle uszkodzone aby uniemożliwić odzyskanie danych;
14. przeprowadzenie co najmniej raz w ciągu roku kalendarzowego szkolenia z pracownikami UG z zakresu ochrony danych osobowych;
15. przedstawianie administratorowi danych osobowych do 31 grudnia każdego roku kalendarzowego pisemnej analizy dotyczącej stanu przestrzegania w UG przepisów o ochronie danych osobowych, mogących wystąpić w tym zakresie zagrożeniach oraz wniosków do dalszej działalności
16. przeprowadzenie szkolenia z zakresu ochrony danych osobowych z każdym nowo zatrudnionym pracownikiem;
17. udziałów szkoleniach specjalistycznych.

§4

Sekretarz Gminy w zakresie ochrony danych osobowych, odpowiada za:

1. na podstawie przedstawionych przez pracowników UG wniosków, zgłaszanie zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, po wcześniejszym ich uwierzytelnieniu przez administratora danych;
2. prowadzenie w UG ewidencji osób upoważnionych do przetwarzania danych osobowych, zgodnie z wymogami art. 39 „ustawy";
3. przedstawianie do podpisu administratorowi danych upoważnień dla pracowników przeznaczonych do przetwarzania danych, po wcześniejszym zgłoszeniu tych zbiorów do rejestracji w GIODO;
4. dopilnowanie aby pracownicy upoważnieni do przetwarzania danych osobowych z poszczególnych zbiorów, mieli to zadanie odnotowane w zakresach swoich obowiązków służbowych;
5. na podstawie przedstawionych przez pracowników UG wniosków, zgłaszanie GIODO każdej zmiany informacji o której mowa w art.41 ust.1 „ustawy", w terminie 30 dni od dnia dokona nia zmiany w zbiorze danych.

§5

Pracowników UG upoważnionych do przetwarzania danych osobowych zobowiązuję do:

1. ścisłego przestrzegania przepisów prawa w zakresie ochrony danych osobowych do których przetwarzania zostali uprawnieni, w tym zaleceń zawartych w „Polityce bezpieczeństwa" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";
2. zachowania w tajemnicy dane osobowe do których przetwarzania zostali upoważnieni oraz sposoby ich zabezpieczenia;
3. przedstawiania Sekretarzowi Gminy wniosków zgłoszenia zbioru danych, który na podstawie przeprowadzonej analizy nowo opublikowanych aktów prawnych, należy zgłosić do rejestracji GIODO, przed zapoczątkowaniem jego przetwarzania w zakresie wynikającym z tych przepisów;

4. przedstawiania Sekretarzowi Gminy wniosków zgłoszenia każdej zmiany informacji o której mowa w art.41 ust.1 „ustawy", w celu zgłoszenia GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. i
5. bieżącego usuwania z używanych systemów informatycznych danych osobowych przetwarzanych wyłącznie w celu edycji tekstu;
6. zmiany nie rzadziej niż co 30 dni hasła uwierzytelniającego użytkownika przetwarzającego dane w systemie informatycznym;
7. niezwłocznego poinformowania administratora bezpieczeństwa o utracie tzw. tożsamości elektronicznej(tj. danych służących uwierzytelnieniu) w celu jak najszybszego uniemożliwienia pozyskania danych przez osoby nieuprawnione;
8. szczególnej ochrony miejsca przetwarzania danych przed dostępem osób nieupoważnionych w celu uniknięcia zainstalowania oprogramowania, które spowoduje przejęcie przez osobę nieuprawnioną danych służących uwierzytelnieniu (identyfikatora i hasła) lub podłączenia w tym celu w sposób niezauważony odpowiednich urządzeń nazywanych keyloggerami;
9. każdorazowego wyrejestrowania się z systemu informatycznego w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba;
10. stosowania wyłącznie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej;
11. każdorazowego zamykania pomieszczeń służbowych, w przypadku czasowego opuszczenia stanowiska pracy, w których przetwarzane są w formie papierowej dane osobowej i nie pozostawiania w nich osób nieuprawnionych, w celu uniemożliwienia wglądu do tych danych albo ich zaboru;
12. wykonywania kopii zapasowych zbiorów przetwarzanych danych, a następnie przechowywania ich wyłącznie w miejscach zabezpieczających przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
13. pozbawienia zapisu danych osobowych w sposób uniemożliwiający ich odzyskanie z urządzeń, dysków lub innych elektronicznych nośników informacji przekazywanych do naprawy;
14. likwidacji nie nadających się do dalszego używania urządzeń, dysków lub innych elektronicznych nośników informacji wyłącznie w obecności powołanej na tą okoliczność przez wójta komisji . Sposób uszkodzenia tych urządzeń powinien uniemożliwić odzyskanie danych;
15. bezpośredniego nadzorowania wykonywanych na terenie budynku UG napraw urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe.

§6

Zwolnienie z obowiązku zgłoszenia zbioru danych osobowych do rejestracji GIODO, które dotyczy zbiorów wskazanych w art. 43 ust. I „ustawy" , nie zwalnia użytkowników tych danych od ich zabezpieczenia, o którym mowa w art. 36 „ustawy" oraz §5 niniejszego zarządzenia.

§7

Wykonanie zarządzenia powierza się Inspektorowi Bezpieczeństwa Informacji.

§8

Traci moc zarządzenie nr 01152.46.2010 Wójta Gminy Ślemień z dnia 08 czerwca 2010 roku w sprawie organizacji przetwarzania danych osobowych przez pracowników Urzędu Gminy w Ślemieniu.

§9

Zarządzenie wchodzi w życie z dniem jego podpisania.

W Ó J T

Andrzej Piecha