

ZARZĄDZENIE NR 12/2017
WÓJTA GMINY ROGÓŹNO

z dnia 26 stycznia 2017 r.

**w sprawie ustalenia „Planu sprawdzeń zgodności przetwarzania danych osobowych
z przepisami o ochronie danych osobowych na rok 2017 w Urzędzie Gminy Rogóźno”**

Na podstawie art. 36a ust 9 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) w związku z rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r. poz. 745) ustalam, co następuje:

§ 1. 1. Wprowadzam do użytku „Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych na rok 2017 w Urzędzie Gminy Rogóźno ” dotyczący ochrony danych osobowych stanowiący załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy Rogóźno.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójta
z dnia 27 stycznia 2017 r.

Gminy

Rogóżno

Plan sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych na okres od dnia 1 stycznia 2017 r. do dnia 31 grudnia 2017r.

§ 1. Przedmiotem sprawdzenia jest zgodność zasad przetwarzania danych osobowych obowiązujących w Urzędzie Gminy Rogóżno z przepisami ustawy o ochronie danych osobowych.

§ 2. Sprawdzenie obejmuje w szczególności:

- 1) opracowania i kompletności dokumentacji przetwarzania danych;
- 2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
- 3) stanu faktycznego w zakresie przetwarzania danych osobowych;
- 4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzanych danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
- 5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

§ 3. Zakres sprawdzeń i ich szczegółowa tematyka dotyczy:

- 1) zgodności opracowanej polityki bezpieczeństwa oraz instrukcji zarządzania systemami informatycznymi z obowiązującymi przepisami;
- 2) posiadania upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zapoznaniu się z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych;
- 3) prowadzonej ewidencji wydanych upoważnień i jej zgodności z wydanymi upoważnieniami;
- 4) stosowania w praktyce zasad określonych w polityce bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych, instrukcji zarządzania systemem informatycznym, zasadach korzystania z komputerów służbowych oraz ochrony własności intelektualnej;
- 5) ustawienia sprzętu komputerowego w pomieszczeniach, pod względem uniemożliwienia dostępu do ekranów monitorów osobom postronnym;
- 6) zabezpieczenia dokumentów zawierających dane osobowe (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym);
- 7) przestrzeganie przez pracowników procedur związanych z zabezpieczeniem danych w trakcie pracy (na podstawie rozmów z pracownikami i obserwacji);
- 8) sposobu niszczenia niepotrzebnych dokumentów;

- 9) dostępu pracowników do zbioru danych oraz zakres dostępu pracownikowi i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień);
- 10) legalności przetwarzania danych osobowych poprzez spełnienie warunków określonych w art. 23 ust. 1 ustawy);
- 11) obowiązku informacyjnego wynikającego z art. 24 ustawy;
- 12) respektowania praw osób, których dane są przetwarzane (rozdział 4 ustawy);
- 13) przestrzegania zasad nadawania/zmieniania/odbierania uprawnień do systemów informatycznych;
- 14) przestrzegania zasady rozpoczęcia i zakończenia pracy w systemie;
- 15) blokowania systemu, podczas opuszczenia stanowiska pracy w trakcie dania pracy;
- 16) poziomu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi;
- 17) stosowania identyfikatorów i haseł dla użytkowników;
- 18) zabezpieczenia systemowego i fizycznego sprzętu komputerowego;
- 19) tworzenia kopii zapasowych;
- 20) odnotowywanie przez systemy służące przetwarzaniu danych osobowych czynności wykonanych przez użytkowników.

§ 4. Ustala się wykaz pomieszczeń i stanowisk podlegających sprawdzeniu z zakresu ochrony danych:

Lp.	Referat/stanowisko podlegające kontroli	przedmiot sprawdzenia	Zakres sprawdzenia	Termin sprawdzenia	Sposób i zakres dokumentowania sprawdzeń
1	Referat Finansowy: stanowisko do spraw poboru zobowiązań pieniężnych i spraw finansowych	Zbiór danych: Podatki i opłaty lokalne	zgodnie z § 3 niniejszego planu sprawdzeń	maj 2017	sprawozdanie
2	Urząd Stanu Cywilnego	Zbiór danych: USC- rejestry małżeństw, zgonów, urodzeń ŹRÓDŁO	zgodnie z § 3 niniejszego planu sprawdzeń	kwiecień 2017	sprawozdanie
3	Referat Organizacyjny Stanowisko obsługi kancelaryjnej	Zbiór danych: Rejestr skarg i wniosków	zgodnie z § 3 niniejszego planu sprawdzeń	kwiecień 2017	sprawozdanie
4	Referat Gospodarki i Rozwoju stanowisko do spraw utrzymania czystości porządku w gminie oraz gospodarki odpadami	Zbiór danych: opłata za gospodarowanie odpadami komunalnymi	zgodnie z § 3 niniejszego planu sprawdzeń	październik 2017	sprawozdanie
5	Referat Organizacyjny stanowisko spraw obrony cywilnej,	Zbiór danych: dodatki mieszkaniowe	zgodnie z § 3 niniejszego planu sprawdzeń	czerwiec 2017	sprawozdanie

	wojskowych i dodatków mieszkaniowych				
6	Referat Organizacyjny stanowisko spraw obrony cywilnej, wojskowych i dodatków mieszkaniowych	Zbiór danych: Ewidencja przedpoborowych i poborowych	zgodnie z § 3 niniejszego planu sprawdzeń	kwiecień 2017	sprawozdanie
7	Samodzielne stanowisko do spraw zamówień publicznych i gospodarki komunalnej	Zbiór danych: Zamówienia publiczne	zgodnie z § 3 niniejszego planu sprawdzeń	październik 2017	sprawozdanie

Sporządził:

Zatwierdził:

.....

.....

Administrator Bezpieczeństwa
Informacji