

ZARZĄDZENIE NR 9/2018
WÓJTA GMINY ROGÓŻNO

z dnia 5 lutego 2018 r.

**w sprawie ustalenia planu sprawdzeń zgodności przetwarzania danych osobowych
z przepisami o ochronie danych osobowych na 2018 rok w Urzędzie Gminy Rogóżno**

Na podstawie art. 36a ust 2 pkt 1 lit.a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.) 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) ustalám, co następuje:

§ 1. 1. Wprowadzam do użytku „Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych na rok 2018 w Urzędzie Gminy Rogóżno ” dotyczący ochrony danych osobowych stanowiący załącznik do niniejszego zarządzenia.

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

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych na 2018 rok

§ 1. Przedmiotem sprawdzenia jest zgodność zasad przetwarzania danych osobowych 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 dnia 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	Sposób i zakres dokumentowania sprawdzeń
1	Referat Organizacyjny, Referat Finansowy, referat Gospodarki i Rozwoju Gminy	Dokumenty zawierające dane osobowe sprzęt komputerowy	zabezpieczenia dokumentów zawierających dane osobowe(czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym ustawienia sprzętu komputerowego w pomieszczeniach, pod względem uniemożliwienia dostępu do ekranów monitorów osobom postronnym przestrzeganie przez pracowników procedur związanych z zabezpieczeniem danych w trakcie pracy	I kwartał	(na podstawie rozmów z pracownikami i obserwacji

2	Urząd Stanu Cywilnego	Dokumenty zawierające dane osobowe sprzęt komputerowy	zabezpieczenia dokumentów zawierających dane osobowe (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym) ustawienia sprzętu komputerowego w pomieszczeniach, pod względem uniemożliwienia dostępu do ekranów monitorów osobom postronnym przestrzeganie przez pracowników procedur związanych z zabezpieczeniem danych w trakcie pracy		(na podstawie rozmów z pracownikami i obserwacji
3	Samodzielne stanowisko do spraw gospodarki komunalnej i zamówień publicznych	Dokumenty zawierające dane osobowe sprzęt komputerowy	zabezpieczenia dokumentów zawierających dane osobowe (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym) ustawienia sprzętu komputerowego w pomieszczeniach, pod względem uniemożliwienia dostępu do ekranów monitorów osobom postronnym przestrzeganie przez pracowników procedur związanych z zabezpieczeniem danych w trakcie pracy	II kwartał	(na podstawie rozmów z pracownikami i obserwacji
4	Informatyk Urzędu Administrator Systemów Informatycznych	Serwerowania, dyski, płyty CD pendrive	poziomu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi; stosowania identyfikatorów i haseł dla użytkowników; zabezpieczenia systemowego i fizycznego sprzętu komputerowego; tworzenia kopii zapasowych; odnotowywanie przez systemy służące przetwarzaniu danych osobowych czynności wykonanych przez użytkowników.	III kwartał	na podstawie sprawdzenia liczby kopii zapasowych, rejestru haseł , systemów zabezpieczeń, obserwacji , rozmów z ASI

Sporządził:

Zatwierdził:

Administrator Bezpieczeństwa

Informacji