Wójt Gminy
Chojnów
woj. dolnośląskie

Zarządzenie nr 0050.101.2016
Wójta Gminy Chojnów
z dnia 15 grudnia 2016r.r.

w sprawie planu sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych.

Na podstawie Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 poz. 745) zarządzam co następuje:

§ 1

Powołuję zespół kontrolny w składzie:

1) Honorata Tajchman-Rękoś - Administrator Bezpieczeństwa Informacji w Urzędzie Gminy Chojnów,
2) Paweł Sobczyk - Administrator Systemu Informatycznego w Urzędzie Gminy Chojnów.

§ 2

Zatwierdzam plan sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych przedstawiony przez administratora bezpieczeństwa informacji zgodnie z § 5 Rozporządzenia, stanowiący załącznik do niniejszego zarządzenia.

§ 3

Zobowiązuje zespól kontrolny po przygotowania sprawozdania po zakończeniu każdego z planowanych sprawdzeń.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Z up. WÓJTA
mgr Honorata Tajchman-Rękoś
SEKRETARZ GMINY

Załącznik nr 1
do Zarządzenia nr
0050.101.2016
Wójta Gminy Chojnów
z dnia 15.12.2016 r.

Plan sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych na okres od 1 stycznia do 31 grudnia 2016r.

Plan sprawdzeń sporządzony zgodnie z §3 ust. 2 pkt. 1 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

Przedmiotem sprawdzenia jest zgodność zasad przetwarzania danych osobowych obowiązujących w UG Chojnów z przepisami o ochronie danych osobowych przeprowadzony raz w roku. Termin przeprowadzenia sprawdzenia miesiąc grudzień 2016.

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 przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

Zakres sprawdzeń i ich szczegółowa tematyka:
1. Zgodność opracowanej polityki bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi z obowiązującymi przepisami.
2. Upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zapoznaniu z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych.
3. Ewidencja wydanych upoważnień oraz jej zgodność z wydanymi upoważnieniami.
4. Stosowanie w praktyce zasad określonych w polityce bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych, instrukcji zarządzania systemem informatycznym, w zasadach korzystania z komputerów służbowych oraz ochrony własności intelektualnej.
5. Ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym.
6. Zabezpieczenie 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 obserwacji oraz rozmów z nimi.
8. Sposób niszczenia niepotrzebnych dokumentów.

9. Dostęp pracowników do zbiorów danych oraz zakres dostępu pracowników i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień).

10. Legalność przetwarzania danych osobowych- spełnianie warunków postawionych w art. 23. ust.1 ustawy.
11. Obowiązek informacyjny wynikający z art. 24 ustawy.
12. Respektowane praw osób, których dane są przetwarzane (rozdział 4 ustawy).
13. Zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych.
14. Przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie.
15. Blokowanie systemu, podczas opuszczenia stanowiska pracy w trakcie dnia pracy.
16. Upoważnienia osób dopuszczonych do pracy w systemie.
17. Stosowanie identyfikatorów i haseł dla użytkowników zgodnie z wymogami formalnymi.
18. Poziom ochrony systemów informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi.
19. Zabezpieczenie systemowe i fizyczne sprzętu komputerowego.
20. Tworzenie kopii zapasowych.
21. Odnotowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywane na danych osobowych przez użytkowników.

Wykaz pomieszczeń podlegających sprawdzeniu z zakresu ochrony danych:
Pomieszczenia wybierane wyrywkowo w ilości 30%

Sporządził:

(nazwisko i imię ABI)

Z up. WÓJTA
mgr Honorata Tajchman-Rękoś
SEKRETARZ GMINY

Zatwierdzam:

(kierownik jednostki)

WÓJT
mgr Andrzej Pyrz