Załącznik nr 4
do Zarządzenia nr 7/2013
Przewodniczącego Zarządu Związku Gmin Krajny w Złotowie
z dnia 21sierpnia 2013r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. Niniejsza instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w systemie informatycznym Związku Gmin Krajny w Złotowie.
2. Instrukcję stosuje się w przypadku stwierdzenia naruszenia zabezpieczeń sprzętu informatycznego, sieci komputerowej lub zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.
3. W przypadku stwierdzenia naruszenia:
   a) zabezpieczenia systemu informatycznego,
   b) technicznego stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   e) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

   każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji i bezpośredniego przełożonego.
4. Do czasu przybycia Administratora Bezpieczeństwa na miejsce naruszenia ochrony danych osobowych, należy:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
   d) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
   e) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   f) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji.
5. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na

RADCA PRAWNY
BCP - 209
Radosław Kilar

Stwierdza się prawidłowość
używanego zabezpieczenia pod względem
formalnoprawnym. Uwagi stanowią załącznik
postępowania.

uwadze ewentualne zagrożenia dla prawidłowości pracy Związku,

b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

c) w razie potrzeby powiadamia o zaistniałym naruszeniu Administratora Danych,

d) jeżeli zasoby systemu na to pozwalają, generuje i drukuje wszystkie raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia,

e) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczeń przed usunięciem śladów naruszenia ochrony danych:

- fizycznie odłącza urządzenie i segmenty sieci, które mogłyby umożliwić dostęp do bazy danych osobie niepowołanej,
- wylogowuje użytkownika podejrzanego o naruszeni ochrony danych,
- zmienia hasła konta administratora i użytkownika, poprze którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu,

f) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń, oraz powiadamia odpowiednie instytucje.

6. Po wyczerpaniu niezbędnych środków doraźnych, Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje działania naprawcze oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii bezpieczeństwa i terminu wznowienia przetwarzania danych.
7. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik A do niniejszego załącznika.
8. Raport, o którym mowa w ust. 7, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych Osobowych (Przewodniczącemu Zarządu), a w przypadku jego nieobecności osobie uprawnionej.
9. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę mającą na celu określenie przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń.