ZARZĄDZENIE NR 42/2013

WOJEWODY ŚWIĘTOKRZYSKIEGO

z dnia 14 maja 2013 roku

w sprawie powołania Administratora Bezpieczeństwa Informacji w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach oraz określenia jego zakresu odpowiedzialności

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.), oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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 2004 r. nr 100, poz. 1024) zarządza się, co następuje:

§ 1.1. Wyznacza się Pana Marka Raka – Informatyka Wojewódzkiego – Kierownika Oddziału ds. Informatyki, Administratorem Bezpieczeństwa Informacji (ABI) w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach.

2. Zadaniem Administratora Bezpieczeństwa Informacji (ABI), o którym mowa w ust. 1 jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach.

§ 2. Administrator Bezpieczeństwa Informacji (ABI) realizuje zadania z zakresu ochrony danych osobowych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych przetwarzanych w Świętokrzyskim Urzędzie Wojewódzkim;
2) podejmowania, stosownych działań zgodnie z przyjętą „Polityką bezpieczeństwa" i „Instrukcją zarządzania systemem informatycznym" służącą do przetwarzania danych osobowych w Świętokrzyskim Urzędzie Wojewódzkim,
3) w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym, niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o naruszeniu przepisów ustawy o ochronie danych osobowych;
4) nadzoru i kontroli nad systemami informatycznymi służącymi do przetwarzania danych osobowych oraz zbiorami papierowymi i osobami przetwarzającymi dane w w/w zbiorach.

§ 3.1. Administrator Bezpieczeństwa Informacji (ABI) realizując swoje zadania współpracuje z Administratorem Danych Osobowych (ADO) i Administratorami Systemów Informatycznych (ASI).

2. Do szczegółowych czynności Administratora Bezpieczeństwa Informacji (ABI) zalicza się w szczególności:

1) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem, poprzez:
   a) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolę przebywających w nich osób,
   b) nadzór nad zarządzaniem hasłami użytkowników, zgodnie z wytycznymi zawartymi w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
   c) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   d) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych wg instrukcji zarządzania systemem informatycznym,
   e) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych
   w przypadku awarii systemu,
   f) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
   g) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
   h) nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,
   i) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego, informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych wg instrukcji

postępowania
w sytuacji naruszenia danych osobowych,

j) analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie administratorowi danych propozycji odpowiednich zmian do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

2) kontrolę dotyczącą, tego kiedy i przez kogo zostały dane osobowe do zbioru wprowadzone oraz komu są przekazywane;
3) opiniowanie wniosków do rejestracji danych osobowych kierowanych do Generalnego Inspektora Ochrony Danych Osobowych;
4) nadzór nad prowadzeniem wymaganej dokumentacji;
5) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz stosowania środków technicznych i organizacyjnych przy przetwarzaniu danych osobowych;
6) nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.

§ 4. Wykonanie zarządzenia powierza się Dyrektorowi Wydziału Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

WOJEWODA ŚWIĘTOKRZYSKI
Bronisława Polka-Koruba