ZARZĄDZENIE NR ORG.0050.50.2015
WÓJTA GMINY JUCHNOWIEC KOŚCIELNY

z dnia 25 czerwca 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji.

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. 2013r., poz. 594 z późn. zm.[1]) i art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2014 r., poz. 1182 z późn. zm.[2]) zarządza się, co następuje:

§ 1. 1. Powołuje się Pana Tomasza Lulkiewicza na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Juchnowiec Kościelny.

2. Zakres działania ABI stanowi załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

mgr Krzysztof Marcinowicz

[1] Zm. poz. 645 i 1318 oraz z 2014 r. poz. 379 i 1072.
[2] Zm. poz. 1662.

Załącznik do Zarządzenia Nr ORG.0050.50.2015

Wójta Gminy Juchnowiec Kościelny

z dnia 25 czerwca 2015 r.

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

Stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

2) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.

3. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia powinny być zasilane poprzez zastosowanie specjalnych urządzeń podtrzymujących zasilanie.

4. Przestrzeganie, aby komputery przenośne, w których przetwarzane są dane osobowe, zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz, aby nie były one udostępniane osobom nieupoważnionym do przetwarzania danych osobowych. Osoby posiadające komputery przenośne z zapisanymi w nich danymi osobowymi nie mają prawa wynosić ich poza obszar budynku Urzędu Gminy Juchnowiec Kościelny.

5. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe. Dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności Administratora Bezpieczeństwa Informacji, a w przypadku nieobecności Administratora Bezpieczeństwa Informacji, osoby upoważnionej przez Administratora Danych Osobowych.

6. Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

7. Nadzorowanie czynności związanych ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.

8. Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.

9. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

10. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny.

11. Nadzór nad funkcjonowaniem mechanizmów uwierzytelnia użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych. Nadzorowanie powinno obejmować:

1) ustalenie identyfikatorów użytkowników i haseł,

2) dopilnowanie, aby hasła użytkowników były zmieniane nie rzadziej niż raz w miesiącu,

3) dopilnowanie, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,

4) dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane, a ich hasła unieważnione.

12. Przestrzeganie, aby jeżeli istnieją odpowiednie możliwości techniczne, ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie się wyłączały po upływie ustalonego czasu nieaktywności użytkownika. Zalecanym rozwiązaniem powyższego problemu jest zastosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchomiają blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła. Wygaszacz taki oprócz ochrony danych, które przez dłuższy czas wyświetlane byłyby na ekranie monitora, chroni system przed przechwyceniem sesji dostępu do danych przez nieuprawnioną osobę.

13. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania o których mowa wyżej powinny mieć na celu wykrycie przyczyn lub sprawcy zaistniałej sytuacji i jej usunięcie. Szczegółowe zasady postępowania w przypadku naruszenia zabezpieczeń są określone w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. W przypadku, gdy na przykład istnieje podejrzenie, iż naruszenie bezpieczeństwa danych osobowych spowodowane zostało zaniedbaniem lub naruszeniem dyscypliny pracy, zadaniem Administratora Bezpieczeństwa Informacji powinno być przedstawienie wniosku Administratorowi Danych Osobowych o wszczęcie postępowania wyjaśniającego i ukaranie odpowiedzialnych za to osób.

14. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeżeli takie nastąpiło) i przygotowanie oraz przedstawienie Administratorowi Danych Osobowych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych. Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek śledzenia skuteczności zabezpieczeń, o których mowa wyżej, oraz obowiązek ich udoskonalania, nałożony na Administratora Bezpieczeństwa Informacji, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

15. Przeszkolenie osób przetwarzających dane osobowe w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych.