ZARZĄDZENIE NR 55/08

WÓJTA GMINY KOŁAKI KOŚCIELNE
z dnia 27 czerwca 2008 r.

w sprawie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie „SOO".

Na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926, Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219, Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708, Nr 104, poz. 711, z 2007 r. Nr 165, poz. 1170) oraz § 3, 4 i 5 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. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Ustala się „Politykę bezpieczeństwa systemu informatycznego służącego do przetwarzania danych osobowych w systemie SOO" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Ustala się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie SOO" stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuję Kierownika USC i osobę zastępującą Kierownika w czasie jego nieobecności, do przestrzegania zasad i realizacji zadań określonych w załącznikach, o których mowa w § 1 i 2.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1

do Zarządzenia Nr 55/08

Wójta Gminy Kołaki Kościelne

z dnia 27 czerwca 2008 r.

POLITYKA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE SOO

§ 1. Niniejszy dokument reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym SOO służącym do wspomagania wydawania dowodów osobistych oraz zbiorów danych zapisanych w postaci papierowej w Urzędzie Stanu Cywilnego w Kołakach Koscielnych.

§ 2. Użyte w „Polityce Bezpieczeństwa" terminy oznaczają:

1) Administrator Danych – Wójta Gminy,

2) Administrator Bezpieczeństwa – Administratora Bezpieczeństwa Informacji wyznaczonego przez Wójta Gminy,

3) użytkownicy systemu - osoby upoważnione do przetwarzania danych osobowych w systemie SOO.

§ 3. Obszarem przetwarzania danych osobowych w systemie SOO jest pomieszczenie USC Nr 26 w budynku Urzędu Gminy Kołaki Kościelne.

§ 4. W systemie informatycznym przetwarzane są dane osobowe zgodnie z wymaganiami ustawy o dowodach osobistych**.**

§ 5. W skład systemu wchodzą:

1) dokumentacja papierowa,

2) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji,

3) wydruki komputerowe.

§ 6. Do przetwarzania danych osobowych w systemie informatycznym SOO zastosowano aplikację bazodanową MSWiA, pracującą pod kontrolą sytemu operacyjnego MS WINDOWS oraz program MSWiA do tworzenia kopii zapasowych**.**

§ 7. Opis struktury zbiorów danych osobowych znajduje się w MSWiA.

§ 8. Informacje z systemu SOO zasilają system informatyczny Wydawania Dowodów Osobistych program firmy MSWiA. Dane są wprowadzane z wydruków, raportów generowanych przez pierwszy z tych systemów.

§ 9. Środki ochrony technicznej:

1) Pomieszczenie, w którym zlokalizowane są obszary przetwarzania danych osobowych jest monitorowane i ma ochronę obiektu w systemie dyskretnego ostrzegania.

2) Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniu, które jest monitorowane.

§ 10. Środki sprzętowe, informatyczne i telekomunikacyjne

1) Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze awaryjne.

2) Niszczenie tymczasowych wydruków papierowych z danymi osobowymi odbywa się przy pomocy niszczarki.

3) Kopie awaryjne wykonywane są przez MSWiA.

§ 11. Środki ochrony w ramach oprogramowania urządzeń teletransmisji

1) Zastosowano firewall na komputerze użytkowników systemu.

2) Zastosowano program antywirusowy na komputerze użytkowników.

§ 12. Środki ochrony w ramach oprogramowania systemu:

1) Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.

2) Zastosowano specjalistyczne oprogramowanie do tworzenia kopii zapasowych.

3) System informatyczny pozwala zdefiniować4) odpowiednie prawa dostępu do zasobów informatycznych systemu.

5) Zastosowano program antywirusowy.

§ 13. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1) Automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia tych danych.

2) Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

3) Ustalono odrębny identyfikator dla każdego użytkownika.

4) Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji.

§ 14. Środki ochrony w ramach systemu użytkowego

1) Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

2) Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony

jest hasłem uruchomieniowym.

§ 15. Środki organizacyjne

1) Do obsługi systemu informatycznego SOO dopuszczane są osoby upoważnione przez Administratora Danych.

2) Osoby upoważnione posiadają stosowny zakres czynności.

3) Przed dopuszczeniem do przetwarzania danych, osoby, o których mowa w pkt 1 odbywają szkolenie dotyczące bezpieczeństwa danych oraz zapoznają się z obowiązującymi w tym zakresie przepisami wewnętrznymi.

4) Osoby przetwarzające dane osobowe składają stosowne oświadczenia o zapoznaniu się z przepisami, odpowiedzialnością za naruszenie obowiązujących zasad oraz zachowaniu tajemnicy, także po ustaniu zatrudnienia.

5) Wyznaczono administratora bezpieczeństwa informacji, który prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych.

6) Ustalono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie SOO, zawierającą m.in. procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

7) Urządzenia informatyczne posiadają książki serwisowe, w których rejestrowane są przypadki awarii systemu, działania konserwacyjne w systemie oraz jego naprawy.

8) W przypadku, gdy zachodzi konieczność9) naprawy sprzętu poza siedzibą urzędu należy wymontować10) z niego nośniki informacji zawierające dane osobowe**.**

11) W przypadku, gdy uszkodzonym elementem jest nośnik informacji, na którym zapisane są dane osobowe, np. dysk twardy, nośnik ten wymontowuje się, a następnie niszczy.

Załącznik Nr 2

do Zarządzenia Nr 55/08

Wójta Gminy Kołaki Kościelne

z dnia 27 czerwca 2008 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE SOO

PODSTAWOWE POJĘCIA

§ 1. Użyte w „Polityce Bezpieczeństwa” terminy oznaczają :

1) Administrator Danych – Wójta Gminy,

2) Administrator Bezpieczeństwa (ABI) – Administratora Bezpieczeństwa Informacji wyznaczonego przez Wójta Gminy,

3) użytkownicy systemu - osoby upoważnione do przetwarzania danych osobowych w systemie SOO

PODSTAWOWE ZASADY NADAWANIA UPRAWNIEŃ W SYSTEMIE SOO

§ 2. 1. Uprawnienia do przetwarzania danych osobowych w systemie SOO nadaje Administrator Danych zgodnie z przydzielonym zakresem czynności pracownika wystawiając imienne upoważnienie określające zakres tego uprawnienia.

2. Upoważnienie, o którym mowa w ust. 1. stanowi załącznik Nr 1 do niniejszej instrukcji.

3. Rejestr nadanych uprawnień prowadzi ABI.

§ 3. Użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych zostaje zapoznany z ustawą o ochronie danych osobowych, polityką bezpieczeństwa oraz instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie SOO, co potwierdza składając do akt osobowych oświadczenie, stanowiące załącznik Nr 2 do niniejszej instrukcji.

§ 4. ABI stwierdzając otrzymanie upoważnienia i złożenie przez pracownika oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych składa zamówienie na mikroprocesorową kartę dostępową do Dyrektora Centrum Personalizacji Dokumentów MSWiA.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE

§ 5. Rozpoczęcie pracy w systemie:

1) Zalogować2) się do system operacyjnego wkładając do czytnika komputera elektroniczną kartę dostępową oraz podając nazwę użytkownika i hasła.

3) Uruchomić4) aplikację SOO podając identyfikator i hasło dostępu do aplikacji.

5) Rozpocząć6) pracę.

§ 6. Podczas każdorazowego opuszczenia stanowiska komputerowego w trakcie pracy w systemie zablokować§ 7. dostęp do danych osobowych poprzez wyjęcie karty dostępowej.

§ 8. Procedura zakończenia pracy w systemie:

1) Zamknąć2) aplikację.

3) Zamknąć4) system.

5) Wyłączyć6) drukarkę i monitor.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORU SOO ORAZ

PRZECHOWYWANIE NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 9. 1. Użytkownicy systemu nie posiadają uprawnień do tworzenia kopii zapasowych – za utworzenie i zabezpieczenie kopii zapasowych odpowiada MSWiA.

2. Wydruki zawierające dane osobowe przechowywane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w metalowych szafach zabezpieczonych zamkami.

3. Wydruki zawierające dane osobowe, co do których nie ma obowiązku przechowywania należy zniszczyć4. przez pocięcie w niszczarce po ich wykorzystaniu.

5. Dane osobowe zapisane w formie papierowej innej niż wydruki z systemu SOO są przechowywane i niszczone na zasadach określonych w pkt.3.

ŚRODKI OCHRONY SYSTEMU SOO

§ 10. Za ochronę antywirusową odpowiada firma WASKO S.A., której CPD MSWiA powierzyło kompleksowy serwis informatyczny dla systemu SOO.

§ 11. Przeglądy i konserwacja systemu informatycznego oraz urządzeń wykonywane są w terminach określonych przez producenta sprzętu.

§ 12. Z czynności określonych w § 10 sporządzane są protokoły, które przechowuje kierownik USC.

ZASADY POSTĘPOWANIA W PRZYPADKU STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE SOO

§ 13. Każdy użytkownik systemu, który poweźmie wiadomość§ 14. w zakresie naruszenia bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie zgłosić§ 15. ten fakt ABI lub w przypadku jego nieobecności Administratorowi Danych.

§ 16. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI lub upoważnionej przez niego osoby, należy:

1) niezwłocznie podjąć2) czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość3) , a następnie uwzględnić4) w działaniu również ustalenie przyczyn lub sprawców.

5) rozważyć6) wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

7) zaniechać8) , o ile to możliwe dalszych planowanych działań które wiążą się z zaistniałym naruszeniem i mogą utrudnić9) udokumentowanie i analizę,

10) podjąć11) inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów komunikatów towarzyszących

naruszeniu,

12) podjąć13) stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,

14) nie opuszczać15) bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub Administratora Danych.

§ 17. ABI lub osoba przez niego upoważniona:

1) przeprowadza postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia i osoby odpowiedzialnej za naruszenie, w tym celu może żądać2) relacji z zaistniałego zdarzenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać3) informacje związane z tym zdarzeniem,

4) podejmuje stosowne działania w celu zabezpieczenia systemu przed ponownym naruszeniem, jeżeli zachodzi taka potrzeba nawiązuje kontakt ze specjalistami świadczącymi serwis informatyczny,

5) powiadamia Administratora Danych o zaistniałej sytuacji.

§ 18. ABI sporządza raport dotyczący naruszenia ochrony danych osobowych w Urzędzie Stanu Cywilnego w Kołakach Kościelnych, którego wzór stanowi załącznik Nr 3 do niniejszej instrukcji.

§ 19. Raport, o którym mowa w § 15 ABI niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności Sekretarzowi Gminy.

§ 20. ABI zleca użytkownikowi systemu sprawdzenie:

1) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,

2) zawartości zbioru danych osobowych,

3) sposobu działania programu,

4) jakości komunikacji w sieci telekomunikacyjnej,

5) obecności wirusów.

§ 21. Po przywróceniu prawidłowego stanu funkcjonowania przeprowadza się analizę stwierdzającą przyczyny naruszenia ochrony danych osobowych w celu podjęcia stosownych kroków eliminujących podobne zdarzenia w przyszłości.

POSTANOWIENIE KOŃCOWE

§ 22. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działań określonych w niniejszej instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek wszczyna się postępowanie dyscyplinarne.

§ 23. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z

niniejszej instrukcji kwalifikowane są jako ciężkie naruszenie obowiązków pracowniczych.

§ 24. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób zapoznanych z niniejszą instrukcją, zgodnie z załącznikiem Nr 4 do instrukcji.

ZałącznikNr 1

do instrukcji zarządzania systemem

informatycznym służącym

do przetwarzania danych

osobowych w systemie SOO

Kołaki Kościelne, dnia
……..

Pan/i
……
….
……
….

UPOWAŻNIENIE Nr …….
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. 101, poz. 926 z późn. zm.) z dniem …….. upoważniam Pana/ią do dostępu do danych osobowych zawartych w dokumentacji z zakresu:
…… w wersji papierowej i w systemie informatycznym w pełnym zakresie dostępu do danych (przeglądanie, wprowadzanie, modyfikowanie i usuwanie).

Zgodnie z art. 39, ust. 2 wyżej wymienionej ustawy jest Pani zobowiązana do zachowania w tajemnicy, również po ustaniu zatrudnienia, danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz sposobów ich zabezpieczania.

Upoważnienie jest ważne na czas nieokreślony. Upoważnienie wygasa z chwilą jego pisemnego cofnięcia albo rozwiązania stosunku pracy.

Przyjęłam do wiadomości
i wykonania:

…….

Kołaki Kościelne, dnia ……..

ZałącznikNr 2

do instrukcji
zarządzania
systemem

informatycznym
służącym

do przetwarzania
danych

osobowych w
systemie SOO

……..…….. Kołaki Kościelne, dnia

……..…….
/imię i nazwisko pracownika/

……
/stanowisko /

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:

1/. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
2/. polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie SOO stanowiących załączniki Nr 1 i 2 do Zarządzenia Nr 55/08 Wójta Gminy Kołaki Kościelne z dnia 27 czerwca 2008 r.

Świadoma/y odpowiedzialności dyscyplinarnej i karnej oświadczam, że zobowiązuję się do ich przestrzegania oraz zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia także po ustaniu okresu zatrudnienia.

……..

.

/czytelny podpis pracownika/

……

….. / podpis osoby przyjmującej

oświadczenie, stanowisko służbowe/

ZałącznikNr 3

do instrukcji zarządzania systemem

informatycznym służącym

do przetwarzania danych

osobowych w systemie SOO

RAPORT DOTYCZĄCY NARUSZENIA OCHRONY DANYCH OSOBOWYCH
W USC Kołaki Kościelne

1. Data: ……. Godzina : ……
2. Osoba powiadamiająca o zaistniałym zdarzeniu: ……
/imię i nazwisko, stanowisko służbowe/
3. Lokalizacja zdarzenia: ……..
/np. nr pokoju, pomieszczenia,/
4. Rodzaj naruszenia ochrony danych osobowych oraz okoliczności towarzyszące: ……
5. Przyczyny wystąpienia zdarzenia: ……

…….…
……
……..
……
……..……
……..…
6. Podjęte działania:
……
…….…
……
……..……
……..…...……
……..
7. Postępowanie wyjaśniające:
…….
…….…
……..…
……..

……..……..……..…
/data, podpis Administratora Bezpieczeństwa Informacji/

ZałącznikNr 4

do instrukcji zarządzania systemem

informatycznym służącym

do przetwarzania danych

osobowych w systemie SOO

WYKAZ OSÓB ZAPOZNANYCH Z POLITYKĄ BEZPIECZEŃSTWA i INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE SOO

Lp.	Imię i Nazwisko	Stanowisko	Data	Czytelny podpis
