ZARZĄDZENIE nr 516/10

Wójta Gminy Parzęczew

z dnia 30 lipca 2010 r.

w sprawie wprowadzenia do użytku służbowego „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Parzęczewie”

Na podstawie § 4 oraz § 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) zarządza się, co następuje:

§ 1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Parzęczewie” w brzmieniu stanowiącym Załącznik nr 1 do Zarządzenia.

§ 2. Zobowiązuje się pracowników przetwarzających dane osobowe do przestrzegania przepisów dokumentu, o którym mowa w § 1.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1
do Zarządzenia Nr 516/2010
Wójta Gminy Parzęczew
z dnia 30 lipca 2010 r.

Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Parzęczewie

Wprowadzenie

1) Wprowadzenie Polityki Bezpieczeństwa jest wymogiem ustawowym i jest regulowana następującymi aktami prawnymi:
    a) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
    b) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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.
    c) rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433)

2) Polityka bezpieczeństwa ochrony danych osobowych jest zestawem reguł i praw regulujących sposób zarządzania, przetwarzania, przechowywania i dystrybucji danych osobowych ze zbiorów pozostających w Urzędzie Gminy w Parzęczewie.
3) Celem polityki bezpieczeństwa jest zapewnienie maksymalnego poziomu bezpieczeństwa procesu przetwarzania danych osobowych i ochrony przed nieuprawnionym dostępem i ich modyfikacją, utratą poufności przy zachowaniu integralności i rozliczalności danych, poprzez właściwą organizację oraz wprowadzenie i realizację odpowiednich działań przy wykorzystaniu środków technicznych.
4) Niniejsza Polityka bezpieczeństwa zawiera w szczególności:
    a) wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
    b) wykaz zbiorów danych osobowych,
    c) opis struktury zbiorów, środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

5) Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
    a) stwierdzono naruszenie zabezpieczeń systemu informatycznego,
    b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

6) Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędzie Gminy w Parzęczewie,
7) Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w Urzędzie Gminy w Parzęczewie,
8) Administratorem Danych jest Wójt Ryszard Nowakowski.
9) Administrator Danych jest jednocześnie Administratorem Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędzie Gminy w Parzęczewie,
10) Administrator Danych - Administrator Bezpieczeństwa Informacji realizuje zadania z zakresu ochrony danych a w szczególności:
    a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych,

b) podejmowanie stosownych działań zgodnie z niniejszą Polityką Bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
c) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

Rozdział II
Opis zdarzeń naruszających ochronę danych osobowych

Zdarzeniami naruszającymi ochronę danych osobowych bądź stwarzającymi podejrzane naruszenia zabezpieczeń tych danych mogą być następujące przypadki:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.,
2) Niewłaściwe parametry środowiska, takie jak np. nadmierna wilgotność, zbyt wysoka temperatura, oddziaływanie pola elektromagnetycznego,
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na celowe działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
4) Komunikaty alarmujące o próbie naruszenia zabezpieczeń systemu, który zapewnia ochronę danych bądź komunikaty o podobnym znaczeniu,
5) Odstępstwa od prawidłowego stanu danych wskazujące na niewłaściwe działanie systemu i niepożądaną jego modyfikację,
6) Naruszenie lub próba naruszenia integralności systemu baz danych w tym systemie,
7) Modyfikacja lub próba modyfikacji danych oraz zmiana w strukturze danych dokonana bez odpowiedniego upoważnienia (autoryzacji),
8) Stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie,
9) Ujawnienie danych osobowych lub objętych tajemnicą procedur ochrony danych osobowych osobom nieupoważnionym, bądź innych elementów systemu zabezpieczeń,
10) Funkcjonowanie sieci komputerowej lub praca systemu wykazuje nieprzypadkowe odstępstwo od prawidłowego rytmu pracy wskazujące na zaniechanie lub przełamanie ochrony danych osobowych - np. praca w sieci lub przy komputerze osoby do tego nieupoważnionej, sygnał o nieautoryzowanym logowaniu, itp.,
11) Ujawnienie istnienia nieautoryzowanych kont dostępu do danych objętych ochroną,
12) Zniszczenie lub podmiana nośnika z danymi osobowymi bądź skasowanie lub skopiowanie danych osobowych w sposób niedozwolony lub przez osobę nieupoważnioną,
13) Rażące naruszenie dyscypliny pracy w zakresie przestrzeganie procedur bezpieczeństwa informacji np. nie wylogowanie się z systemu przed opuszczaniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero nie wykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych, itp.,
14) Stwierdzenie nieprawidłowości w zakresie zabezpieczania miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.,

Rozdział III
Zabezpieczenie danych osobowych

1) Obszar, w którym przetwarzane są dane osobowe stanowi budynek Urzędzu Gminy w miejscowości Parzęczew, ul. Południowa 1.

2) Wykaz zbiorów danych osobowych ze wskazaniem formy przetwarzania tych danych stanowi załącznik nr 2 do Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy w Parzęczewie.
3) Budynek przy ul. Południowej 1, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany przez pracowników po zakończeniu pracy. Budynek zabezpieczony jest systemem antywłamaniowym.
4) Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.
5) Zbiory danych przetwarzane w postaci tradycyjnej są przechowywane w szafach zamykanych na klucz.
6) Przebywanie osób trzecich w pomieszczeniach, gdzie są przetwarzane dane osobowe dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych lub w obecności przełożonego.
7) Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych, w sposób uniemożliwiający do nich osób trzecich,
8) W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane,
9) Na poziomie aplikacji służącej do przetwarzania danych osobowych zastosowano identyfikator i hasło dostępu dla upoważnionego pracownika,
10) Stacje robocze, z których możliwy jest dostęp do danych zabezpieczony jest hasłem.

Rozdział IV
Gromadzenie, przepływ oraz opis struktury zbiorów danych osobowych

1) Dane osobowe pozyskiwane są z danych źródłowych i innych zasobów. Dane te gromadzone są w systemach informatycznych, zbiorach manualnych oraz zewnętrznych nośnikach danych,
2) Rozwiązania techniczne stosowane w Urzędzie Gminy w Parzęczewie pozwalają na uzupełnienie tych samych danych z innych posiadanych zasobów w ramach jednostki, co służy efektywniejszemu ich wykorzystaniu w załatwianiu spraw,
3) Przepływ danych następuje w sposób manualny przy wykorzystywaniu zewnętrznych nośników danych,
4) Korespondencja z adresatami jest realizowana za pośrednictwem poczty,
5) Gromadzone dane osobowe są udostępniane pracownikom w zakresie niezbędnym do ich pracy,
6) Zakres gromadzonych danych osobowych jest zgodny z przepisami prawa.

Rozdział V
Postępowanie w przypadku naruszenia ochrony danych osobowych

1) W przypadku stwierdzenia naruszenia ochrony danych osobowych każda osoba zatrudniona przy przetwarzaniu tych danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Danych lub upoważnionej osoby,
2) Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych lub upoważnionej osoby, należy:

    - Niezwłocznie podjąć czynności niezbędnego powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
    - Rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
    - Zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowanie i analizę,
    - Podjąć inne stosowne działania przewidziane w instrukcjach technicznych i technologicznych, dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej właściwe dla objawów i sytuacji towarzyszącej naruszeniu,
    - Udokumentować wstępnie zaistniałe zdarzenie,
    - Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych lub upoważnionej osoby,

3) Po przybyciu na miejsce Administrator Danych lub osoby upoważnionej:
    - Zapoznanie się z zaistniałą sytuacją, identyfikuje rodzaj zaistniałego zdarzenia i dokonuje wyboru metody dalszego postępowania celem powstrzymania lub ogranicza dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia śladów naruszenia ochrony danych osobowych,
    - Może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również innych osób mogących posiadać informacje związane z zaistniałym zdarzeniem
    - Rozważa celowość i potrzebę poinformowania o zaistniałym zdarzeniu Administratora Danych
    - W przypadku potrzeby nawiązuje bezpośredni kontakt ze specjalistami spoza Urzędu Gminy w Parzęczewie.

4) Administrator Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać:
    - Wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem
    - Określenie czasu i miejsca naruszenia i powiadomienia
    - Określenie okoliczności towarzyszących i rodzaju naruszenia
    - Wybór metody postępowania wraz z opisem podjętych działań i przesłanek skłaniających do ich podjęcia
    - Wstępną ocenę przyczyn wystąpienia naruszenia
    - Ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego

5) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzanych danych.

6) Zaistniałe zdarzenie powinno stać się przedmiotem szczegółowej analizy przeprowadzonej przez Administratora Danych,
7) Analiza powinna zawierać ocenę zaistniałego zdarzenia, wskazanie osób odpowiedzialnych oraz wnioski nt. ewentualnych przedsięwzięć proceduralnych, organizacyjnych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział VI Postanowienie końcowe

1) Urząd Gminy w Parzęczewie przetwarza dane osobowe na podstawie przepisów prawa.
2) Dane osobowe mogą być udostępniane zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DZ.U. z 2001 r. Nr 101, póz. 926 z późn. zm.).
3) Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się i stosowania zapisów niniejszego dokumentu oraz przepisów ustawy o ochronie danych osobowych.

Załącznik Nr l
do Polityki bezpieczeństwa
w Urzędzie Gminy w Parzęczewie

Wykaz pomieszczeń w których przetwarzane są dane osobowe, opis systemów informatycznych w Urzędzie Gminy w Parzęczewie.

Nr pokoju	**Komórka organizacyjna**	**System**
1	Urząd Stanu Cywilnego	Windows XP Home Edition
3	Referat Funduszy Europejskich	2 x Windows 2000 Windows HP Home Edition
4	Referat Finasów (zasiłki rodzinne)	2 x Windows XP Home Edition
7	Ewidencja Ludności, Zezwolenia na Działalność Gospodarczą, Oświata	2 x Windows 2000 Windows Vista
10	Referat Finansów (płace, roboty publiczne)	3 x Windows 2000
11	Kasa	Windows 2000
12	Referat Finansów (podatki lokalne)	Windows 2000 Windows Xp Home Edition
13	Referat Finansów (księgowość)	2 x Windows 2000
14	Referat Finansów (księgowość oświaty)	Windows 2000 Windows XP Home Edition
19	Skarbnik	Windows XP Home Edition

Załącznik Nr 2
do Polityki bezpieczeństwa
w Urzędzie Gminy w Parzęczewie

Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych.

Nazwa zbioru (opis)	**Program do przetwarzania**
Fundusze EU	3 x Windows 2000, OpenOffice 2 x Windows XP Home Edition, OpenOffice
USC	Windows XP Home Edition, Radix USC+
Ewiencja Ludności	Windows 2000, Radix ELUD Windows Vista, Radix ELUD
Zezwolenia na Działalność Gospodarczą	Windows 2000, Ewidencja Działalności Gospodarczej firmy Info-System
Oświata	Windows 2000, SIO
Zasiłki rodzinne	Windows XP Home Edition, Świadczenia Rodzinne firmy Sygnity
Środki transportowe	Windows XP Home Edition, Auta firmu Info-System
Księgowość Budżetowa	2x Windows 2000, Windows XP Home Edition, Księgowość Budżetowa firmy Info-System
Bankowość Elektroniczna	Windows 2000, KREZUS 3 x Windows XP Home Edition, KREZUS
Podatki lokalne	2 x Windows XP Home Editin, Podatki Lokalne firmy Info-System
Kadry i Płace	3 x Windows 2000, Kadri i Płace firmy Info-System
Płatnik (ZUS)	Windows 2000, Płatnik