Zarządzenie Nr 44/15
Wójta Gminy Pszczółki
z dnia 18 września 2015 roku

w sprawie wprowadzenia i stosowania dokumentacji opisującej sposób przetwarzania danych osobowych w Urzędzie Gminy w Pszczółkach.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z póź. Zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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

Wprowadzam do stosowania Politykę Bezpieczeństwa, stanowiącą załącznik do Zarządzenia.

§ 2

Wprowadzam do stosowania Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, stanowiącą załącznik nr 7 do Polityki Bezpieczeństwa.

§ 3

Zobowiązuje się pracowników Urzędu Gminy do zapoznania się z treścią i przestrzegania postanowień zawartych w wyżej wymienionej dokumentacji.

§ 4

Traci moc Zarządzenie Nr 6/06 Wójta Gminy Pszczółki z dnia 18 stycznia 2006 r.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania i podlega ogłoszeniu w Biuletynie Informacji Publicznej oraz na gminnych tablicach ogłoszeń.

Publikacji nie podlegają załączniki nr 2, 4, 6 oraz 7 do Polityki Bezpieczeństwa ze względu na wyłączenie jawności informacji.

Załącznik do Zarządzenia Nr 44/15
Wójta Gminy Pszczółki
z dnia 18 września 2015 r.

POLITYKA BEZPIECZEŃSTWA

Administrator Danych – Gmina Pszczółki reprezentowana przez Wójta Gminy Pszczółki

dnia 18.09.2015 r. w Urzędzie Gminy w Pszczółkach

zgodnie z **ROZPORZĄDZENIEM 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. 2004 Nr 100, poz. 1024)
wdraża dokument o nazwie „Polityka Bezpieczeństwa".

Zapisy niniejszej Polityki wchodzą w życie z dniem 18.09.2015 r.

§ 1

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminy w Pszczółkach, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
2. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.
3. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach w formie papierowej oraz w systemach informatycznych.
4. Bez względu na zajmowane stanowisko w Urzędzie Gminy, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. **przetwarzaniu danych -** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację np. nadpisywanie, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

6. **naruszeniu danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych,
7. **poufności** – właściwość zapewniająca, że informacja jest dostępna jedynie osobom upoważnionym,
8. **przetwarzaniu danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
9. **administratorze danych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
10. **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności,
11. **administratorze systemu informatycznego** - rozumie się przez to osobę zatrudnioną w urzędzie na stanowisku związanym z obsługą informatyczną urzędu,
12. **podmiocie** – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową.

§ 3

1. Administrator Danych w Urzędzie Gminy w Pszczółkach wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Zarządzenie nr 89/07 Wójta Gminy Pszczółki z dnia 5 grudnia 2007 r. wyznaczające **Administratora Bezpieczeństwa Informacji** oraz jego zakres obowiązków stanowi **załącznik nr 1 do „Polityki Bezpieczeństwa”.**

2. Administrator Bezpieczeństwa Informacji w zakresie swojego działania w urzędzie podlega bezpośrednio Administratorowi Danych w Urzędzie Gminy w Pszczółkach lub osobie przez niego upoważnionej.

3. Do zakresu działania Administratora Bezpieczeństwa Informacji należy również:
   a) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe,
   b) zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
   c) dopilnowanie aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym zalogowaniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
   d) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   e) nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które zawarte są w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   f) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
   g) nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym

sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania w przypadku awarii systemu,

h) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
i) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
j) nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny,
k) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych,
l) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniach zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
m) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie Administratorowi Danych Osobowych odpowiednich zmian do Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych,
n) koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych osobowych z uwzględnieniem zabezpieczenia systemu informatycznego w urzędzie w tym: proponowanie Administratorowi Danych Osobowych mechanizmów ochrony i środków bezpieczeństwa przetwarzania danych osobowych,
o) ścisła współpraca ze służbami prawnymi i wyznaczonymi pracownikami urzędu w prawnych aspektach procesu przetwarzania danych osobowych,
p) koordynacja wprowadzania poziomów bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym,
q) określanie i nadzór nad wdrażaniem standardów zabezpieczeń,
r) opiniowanie wszelkich zmian zachodzących w procesie przetwarzania danych osobowych, pod kątem ich wpływu na bezpieczeństwo,
s) niezwłoczne reagowanie na incydenty w zakresie bezpieczeństwa systemu informatycznego, informowanie Administratora Danych Osobowych o incydentach i ich skutkach,
t) nadzór nad przestrzeganiem przez pracowników zasad ochrony danych osobowych obowiązujących w urzędzie,
u) monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym i dopasowanie systemu do wymagań prawnych,
v) koordynacja bieżących działań związanych ze szkoleniami pracowników, informowaniem pracowników o zagrożeniach,
w) opracowanie i aktualizowanie „Polityki bezpieczeństwa informacji w Urzędzie Gminy Pszczółki" oraz „Instrukcji zarządzania systemem informatycznym" zgodnie z 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,
x) monitorowanie zaleceń i interpretacji GIODO w zakresie ochrony danych osobowych i implementowanie ich w urzędzie,
y) Administrator Bezpieczeństwa Informacji reprezentuje Administratora Danych Osobowych w obszarach związanych z nadzorowaniem przestrzegania obowiązujących zasad bezpieczeństwa danych osobowych oraz koordynuje procesy związane z zarządzaniem systemem informatycznym, przetwarzającym dane osobowe w aspekcie

ich bezpieczeństwa,

§ 4

O naruszeniu ochrony danych osobowych mogą świadczyć symptomy występując w następujących obszarach:

1. w obrębie pomieszczeń, szaf lub miejsc przechowywania:
   a) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych , w szczególności do serwerowni oraz kas, gdzie przechowuje są nośniki kopii zapasowych,
   b) włamanie lub próby włamania do szaf, w których przechowywane są w postaci elektronicznej lub papierowej , nośniki danych osobowych,
2. w obrębie sprzętu informatycznego:
   a) kradzież komputera, w którym przechowywane są dane osobowe,
   b) rozkręcona obudowa komputera,
3. w obrębie systemu informatycznego i aplikacji:
   a) brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych,
   b) brak możliwości zalogowania się do tej aplikacji,
   c) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych),
   d) poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych (na przykład wgląd do szerszego zakresu danych o pracownikach),
   e) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),
   f) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, pendrive'a itp.),
   g) zagubienie bądź kradzież nośnika z zawartością danych osobowych.

4. Każda osoba, która zauważyła niepokojące zdarzenie, wystąpienie powyżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania: bezpośredniego przełożonego i Administrator Bezpieczeństwa Informacji.
5. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż ABI, jest ona zobowiązana poinformować o tym fakcie Administratora Bezpieczeństwa Informacji.
6. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w urzędzie naruszenia bezpieczeństwa danych osobowych, Administrator Bezpieczeństwa Informacji, jest zobowiązany do podjęcia następujących kroków:
   a) stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:

b) sprawdzenia okoliczności zdarzenia,
c) wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich.

7. W przypadku, gdy doszło do naruszenia ochrony danych osobowych:
   a) zebranie ewentualnych dowodów,
   b) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
   c) zabezpieczenia danych przetwarzanych w systemie informatycznym, jego logów systemowych, logów programu i bazy w których nastąpiło naruszenie bezpieczeństwa oraz danych konfiguracyjnych całego systemu w celu późniejszej analizy
   d) usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego tj. stanu sprzed incydentu.

8. System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.
9. Administrator Bezpieczeństwa Informacji określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym urzędu.
10. Administrator Bezpieczeństwa Informacji prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:
    a) imię i nazwisko osoby zgłaszającej incydent,
    b) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
    c) datę zgłoszenia incydentu,
    d) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
    e) wyniki przeprowadzonych działań,
    f) podjęte akcje naprawcze i ich skuteczność.

§ 5

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 2 do „Polityki Bezpieczeństwa”.**

§ 6

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik nr 3 do „Polityki Bezpieczeństwa”.**

§ 7

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa załącznik **nr 4 do „Polityki Bezpieczeństwa”.**

§ 8

Administratora Bezpieczeństwa Informacji oraz pracownicy podmiotu dbają o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny

znajdować się w szafach lub biurkach zamykanym na klucz do których dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 9

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych.** Wzór upoważnienia stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa”**.

2. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie stanowi **załącznik nr 6 do „Polityki Bezpieczeństwa”.**

§ 10

Administrator Bezpieczeństwa Informacji jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 11

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić informacji dotyczących jej danych osobowych.

§ 12

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 13

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje **Instrukcja Zarządzania Systemem Informatycznym** która stanowi **załącznik nr 7 do „Polityki Bezpieczeństwa”**.

§ 14

1. Dostęp do systemu informatycznego, programów przetwarzających dane osobowe oraz urządzeń z nimi powiązanych możliwy jest wyłącznie na podstawie upoważnienia wydanego przez Administratora Danych Osobowych.
2. Przed dopuszczeniem do pracy w systemie informatycznym, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką.
3. Pracownicy przetwarzający dane osobowe obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.

§ 15

1. Ochrona danych osobowych przetwarzanych w urzędzie obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Urzędzie Gminy Pszczółki, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
2. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych

środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.

3. Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych otrzymane od Administratora Danych Osobowych.

4. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

5. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

6. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

7. Zachowanie tajemnicy służbowej obowiązuje pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

8. Administrator Bezpieczeństwa Informacji i Administrator Danych Osobowych są odpowiedzialni za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie urzędu.

§ 16

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. 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.**

Podpis Administratora Danych Osobowych

….....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

….....

Podpis

ZARZĄDZENIE Nr 89/07
WÓJTA GMINY PSZCZÓŁKI
z dnia 5 grudnia 2007 r.

w sprawie wyznaczenia Administratora bezpieczeństwa informacji w Urzędzie Gminy w Pszczółkach

Na podstawie art. 33 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity: Dz. U. z 2001 roku Nr 142 poz. 1591 ze zm.) i art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 roku Nr 101 poz. 926 ze zm.)

Wójt Gminy Pszczółki
zarządza , co następuje:

§ 1

Z dniem 5 grudnia 2007 roku wyznacza się Pana **Rafała Laskowskiego** na Administratora bezpieczeństwa informacji w Urzędzie Gminy w Pszczółkach.

§ 2

Osobę wymienioną w § 1 zobowiązuje się do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 3

Upoważnia się Administratora bezpieczeństwa informacji do nadzoru i kontroli nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych w tut. Urzędzie,

§ 4

Traci moc Zarządzenie Nr 30/06 Wójta Gminy Pszczółki z dnia 19 maja 2006 r. w sprawie wyznaczenia Administratora bezpieczeństwa informacji w Urzędzie Gminy w Pszczółkach.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

załącznik nr 3 do „Polityki Bezpieczeństwa” zgodnie z § 4 pkt 2 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych	Program zastosowany do przetwarzania danych	Uwagi
1.	Rejestr korespondencji przychodzącej i wychodzącej	-	Dokumentacja w wersji papierowej
2.	Elektroniczny obieg dokumentów	el-Dok	-
3.	Księgi stanu cywilnego	Źródło	-
4.	Oświadczenia o stanie majątkowym	-	Dokumentacja w wersji papierowej
5.	Ewidencja ludności	Elud+	-
6.	Rejestr PESEL	Źródło	
7.	Dowody osobiste	Źródło	-
8.	Lista kobiet i mężczyzn do kwalifikacji wojskowej	-	Dokumentacja w wersji papierowej
9.	Rejestr wyborców	Wyb+	-
10.	Dane osobowe pracowników dla ZUS	Płatnik	-
11.	Akta osobowe	Kadry	-
12.	Płace pracowników	Płace	-
13.	Kontrahenci przelewów	Przelewy	-
14.	Dane zleceniobiorców	Zlecone	-
15.	Kontrahenci kasy	Kasa+	-
16.	Podatnicy podatku i opłat lokalnych oraz płatnicy należności nieopodatkowanych	Wip+	-
17.	Podatnicy podatku rolnego, leśnego i od nieruchomości	Pogrun+	-
18.	Podatnicy podatku od środków transportu	Post+	-
19.	System księgowości budżetowej	Fkb+	
20.	Wnioski i decyzje z ZFŚS	-	Dokumentacja w wersji papierowej
21.	Ewidencja przebiegu pojazdów	-	Dokumentacja w wersji papierowej
22.	Uczestnicy ubezpieczenia grupowego	-	Dokumentacja w wersji papierowej
23.	Ewidencja działalności gospodarczej	Epod	-
24.	Rejestr wydanych zezwoleń na sprzedaż napojów alkoholowych	-	Dokumentacja w wersji papierowej

25.	Płatnicy opłat za wodę i ścieki	Eko+	-
26.	Wypisy i wyrysy z miejscowego planu zagospodarowania przestrzennego	-	Dokumentacja w wersji papierowej
27.	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	-	Dokumentacja w wersji papierowej
28.	Rejestr wydanych decyzji o lokalizacji inwestycji celu publicznego	-	Dokumentacja w wersji papierowej
29.	Ewidencja miejscowości, ulic i adresów	-	Dokumentacja w wersji papierowej
30.	Rejestr zatwierdzonych podziałów nieruchomości	-	Dokumentacja w wersji papierowej
31.	Rejestr prowadzonych rozgraniczeń nieruchomości	-	Dokumentacja w wersji papierowej
32.	Rejestr wnioskodawców o przyłączenie do sieci wodociągowej i kanalizacyjnej	-	Dokumentacja w wersji papierowej
33.	Rejestr dzierżawców, użytkowników wieczystych i najemców lokali	-	Dokumentacja w wersji papierowej
34.	Płatnicy opłat adiacenckich i planistycznych	-	Dokumentacja w wersji papierowej
35.	Najemcy mieszkań komunalnych	Ebud+	-
36.	Właściciele nieruchomości objęci gminnym systemem gospodarowania odpadami komunalnymi	Gok+	-
37.	Uczestnicy projektów szkoleniowych z EFS	-	Dokumentacja w wersji papierowej
38.	Wnioskodawcy o przyznanie stypendiów szkolnych	-	Dokumentacja w wersji papierowej
39.	Osoby uprawnione do otrzymania wyprawki szkolnej	-	Dokumentacja w wersji papierowej
40.	Awanse zawodowe nauczycieli	-	Dokumentacja w wersji papierowej
41.	Młodociani pracownicy	-	Dokumentacja w wersji papierowej
42.	Uczniowie korzystający z nauczania indywidualnego	-	Dokumentacja w wersji papierowej
43.	Uczniowie korzystający z dofinansowania do dowozu (w tym niepełnosprawni)	-	Dokumentacja w wersji papierowej
44.	Subskrybenci systemu powiadamiania SMS	mprofi.pl	-
45.	System informacji oświatowej	SIO	-
46.			
47.			
48.			
49.			
50.			
51.			

załącznik nr 5 do „Polityki Bezpieczeństwa”

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....
   o numerze PESEL .....
   zatrudnioną/-ego na stanowisku .....
   w Urzędzie Gminy w Pszczółkach

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (należy określić zbiory zgodnie z załącznikiem numer 3 do Polityki Bezpieczeństwa)

   – .....
   – .....
   – .....
   – .....
   – .....

2. Identyfikator/Login: .....

3. Okres trwania upoważnienia: .....

Wystawił: .....
(podpis Administratora Danych Osobowych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....