ZARZĄDZENIE NR 21/11
WÓJTA GMINY GIBY

z dnia 8 kwietnia 2011 r.

w sprawie ochrony danych osobowych w Urzędzie Gminy w Gibach.

Na podstawie 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. Nr 100, poz. 1024), zarządza się, co następuje:

§ 1. 1. Wprowadza się w Urzędzie Gminy w Gibach (zwanym dalej UG Giby) szczegółowe zasady ochrony danych osobowych, opisane w załącznikach do niniejszego zarządzenia.

2. Wszystkich pracowników UG Giby, a w szczególności przetwarzających dane osobowe, zobowiązuje się do zapoznania z niniejszym zarządzeniem wraz z załącznikami i do przestrzegania zawartych w nim zasad.

3. Osobą odpowiedzialną za zapoznanie wszystkich pracowników UG Giby, a w szczególności przetwarzających dane osobowe, czynię Administratora Bezpieczeństwa Informacji.

§ 2. 1. Przez dane osobowe rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden, lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

2. Przez przetwarzanie danych osobowych rozumie się 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. 1. Przetwarzanie danych osobowych w UG Giby wynika z realizacji zadań statutowych.

2. Przetwarzanie danych osobowych może odbywać się w systemie informatycznym, a także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 4. 1. Administratorem Danych Osobowych, zgodnie z ustawą o ochronie danych osobowych, decydującym o celach i środkach przetwarzania danych osobowych, jest Wójt Gminy Giby.

§ 5. 1. Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji nadzorującego przestrzeganie zasad ochrony danych osobowych w UG Giby.

2. Administrator Bezpieczeństwa Informacji jest upoważniony do wglądu w zbiory i obszary przetwarzania danych osobowych UG Giby.

3. Zadania Administratora Bezpieczeństwa Informacji określone są w Polityce bezpieczeństwa danych osobowych w UG Giby stanowiącej załącznik nr 1 do niniejszego zarządzenia.

§ 6. 1. Ochroną, zabezpieczeniem i kontrolą przetwarzania danych osobowych w systemach informatycznych zajmuje się Administrator Systemu Informatycznego UG Giby, wyznaczony przez Administratora Danych Osobowych.

2. Zadania Administratora Systemu Informatycznego UG Giby w zakresie ochrony danych osobowych określone są w Polityce bezpieczeństwa danych osobowych w UG Giby stanowiącej załącznik nr 1 do niniejszego zarządzenia.

§ 7. 1. Każda osoba, której dane osobowe są przetwarzane, ma prawo do ochrony danych jej dotyczących, do kontroli przetwarzania tych danych oraz do ich ustalenia lub poprawiania, jak również do uzyskiwania wszelkich informacji o przysługujących jej prawach.

2. Osobie wymienionej powyżej, przysługuje prawo do kontroli przetwarzania danych osobowych, które jej dotyczą, zawartych w zbiorach danych, zgodnie z rozdziałem 4 ustawy o ochronie danych osobowych.

3. Osoby, które zostały upoważnione do przetwarzania danych osobowych są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia.

§ 8. 1. Wprowadza się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w UG Giby stanowiącą załącznik nr 2 do zarządzenia.

2. Wprowadza się Instrukcję postępowania w sytuacji naruszania zasad ochrony danych osobowych w UG Giby stanowiącą załącznik nr 3 do zarządzenia.

§ 9. 1. Ustalam wykaz pomieszczeń tworzących w UG Giby obszar, w którym przetwarzane są dane osobowe zgodnie z załącznikiem nr 4 do zarządzenia.

§ 10. 1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, po złożeniu stosownego oświadczenia zgodnie ze wzorem załącznika nr 5 do zarządzenia.

2. Upoważnienie do przetwarzania danych osobowych wydaje Administrator Danych Osobowych na podstawie wniosku zgodnie ze wzorem załącznika nr 6 do zarządzenia.

3. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji zgodnie ze wzorem załącznika nr 7 do zarządzenia.

§ 11. Niniejsze zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Giby

Jan Kramnicz

Załącznik Nr 1 do Zarządzenia Nr 21/11

Wójta Gminy Giby

z dnia 8 kwietnia 2011 r.

Polityka bezpieczeństwa danych osobowych
w Urzędzie Gminy w Gibach.

Rozdział I - Postanowienia ogólne

1. Definicje i skróty

- UG Giby – Urząd Gminy w Gibach,

- Administrator Danych Osobowych (ADO) – Wójt Gminy Giby,

- Administrator Bezpieczeństwa Informacji (ABI) – Sekretarz UG Giby lub inna osoba wyznaczona do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,

- Administrator Systemu Informatycznego (ASI) - Informatyk UG Giby odpowiedzialny za funkcjonowanie systemu informatycznego w UG Giby oraz stosowanie technicznych i organizacyjnych środków ochrony,

- Użytkownik Systemu (US) - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym UG Giby. Użytkownikiem może być pracownik UG Giby, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba wykonująca staż w UG Giby lub wolontariusz,

- sieć lokalna (LAN) - wewnętrzne połączenie systemów informatycznych UG Giby dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

- sieć rozległa (WAN) - siec publiczna w rozumieniu ustawy z dnia 21 lipca 2000r. Prawo Telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.).

2. Zakres

1) Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określa reguły postępowania i czynności praktyczne dotyczące zarządzania, ochrony i dystrybucji informacji podlegającej ochronie (danych osobowych) w UG Giby.

2) Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w UG Giby zawiera:

- identyfikację zasobów systemu informatycznego,

- wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,

- wykaz zbiorów danych osobowych oraz programów zastosowanych do przetwarzania tych danych,

- środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

3. Cele

Celem polityki bezpieczeństwa, o której mowa w pkt. 1, jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki ADO w zakresie zabezpieczenia danych osobowych.

Rozdział II - Identyfikacja zasobów systemu informatycznego

1. Struktura teleinformatyczna UG Giby składa się z przewodowej, strukturalnej sieci lokalnej dołączonej do sieci Internet. W ramach tej struktury funkcjonuje system informatyczny służący do rejestrowania i przetwarzania danych osobowych. Podlega on ochronie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.), zwanej dalej "ustawą".

2. W ramach tej infrastruktury funkcjonuje także system finansowy oraz inne systemy usług sieciowych. Zawierają one dane podlegające ochronie ze względu na powyższą ustawę oraz są strategiczne dla ciągłości pracy i funkcjonowania UG Giby.

3. Podstawowymi systemami informatycznymi w UG Giby są:

- ADAŚ – program obsługujący kadry i płace, ewidencję ludności.
- Xpertis – Podatek rolny, leśny i od nieruchomości ,
- Płatnik - program wymagany do rozliczenia z Zakładem Ubezpieczeń Społecznych,
- Perseus - program finansowo-księgowy,
- Elektroniczna Skrzynka Podawcza - realizowana na platformie Cyfrowy Urząd,
- Elektroniczna Skrzynka Podawcza - realizowana na platformie ePUAP

4. Ze względu na różnorodność systemów i przetwarzanych danych oraz fakt połączenia z globalną siecią Internet, zapewnienie właściwej ochrony systemu informatycznego w UG Giby jest zagadnieniem złożonym.

Rozdział III - Wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych

Przetwarzanie danych osobowych jest wykonywaniem jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zamienianie, udostępnianie i usuwanie, a zwłaszcza takich, które wykonuje się w systemach informatycznych. Biorąc pod uwagę przepisy ustawy, nakazujące jej stosowanie także w przypadkach przetwarzania danych poza zbiorem danych, przetwarzanie danych osobowych może wystąpić w większości pomieszczeń UG Giby. Ze względu jednak na szczególne nagromadzenia danych osobowych, szczególnie chronione powinny być pomieszczenia, w których znajdują się elementy struktury informatycznej przechowujące, przetwarzające i udostępniające dane osobowe (jak serwery baz danych), przechowujące i składujące kopie zapasowe, pomieszczenia archiwów zakładowych oraz pomieszczenia komórek finansowo-księgowych i kadrowych. Szczegółowy spis pomieszczeń, w których przetwarzane są dane osobowe znajduje się w załączniku 6 do zarządzenia..

Rozdział IV - Wykaz zbiorów danych osobowych przetwarzanych w UG Giby:

1) Dokumentacja papierowa (korespondencja, wnioski, deklaracje, itp.),

2) Wydruki komputerowe,

3) Bazy wykorzystywane przez oprogramowanie wskazane w rozdziale drugim.

Rozdział V - Środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych

System informatyczny UG Giby, ze względu na połączenie z siecią publiczną, musi zapewniać środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa (§ 6 ust. 4 rozporządzenia 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).

1. Bezpieczeństwo fizyczne.

Gwarancją zapewnienia bezpieczeństwa systemu informatycznego UG Giby oraz przetwarzanych i przechowywanych danych jest zapewnienie bezpieczeństwa fizycznego. Warunkiem zapewnienia bezpieczeństwa fizycznego systemu jest kontrola dostępu do wszystkich stacji roboczych. W związku z tym szczególną ochroną obejmuje się pomieszczenia, w których znajdują się węzły sieci oraz te, w których przechowywane są i składowane dane. Wymienione pomieszczenia powinny być stale zamknięte, a dostęp do nich powinny mieć tylko upoważnione osoby.

2. Zarządzanie oprogramowaniem.

ADO wyznacza ASI, który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustawowych zadań UG Giby i posiadających ważną licencję użytkowania.

3. Uwierzytelnianie użytkowników.

Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez ASI na wniosek ABI.Dostęp do systemów operacyjnych serwerów i stacji roboczych powinien być chroniony przez nazwę użytkownika i hasło. Zespół ten tworzy jedną z głównych linii obrony przed intruzami. Dlatego należy uświadamiać użytkownikom rolę, jaką w systemie ochrony odgrywa dobrze wybrane i trudne hasło o odpowiednio dobranym czasie życia (wygaśnięcia). Jednocześnie należy wdrożyć mechanizmy systemowe kontrolujące składnię i czas życia haseł. System powinien mieć wbudowane mechanizmy ograniczające liczbę błędnych prób logowania oraz umożliwiające wskazanie stacji roboczych, na których dany użytkownik może pracować. Zalecane jest ustawienie blokady konta użytkownika na 3 do 5 prób logowania.

Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika, ani jego imieniem lub nazwiskiem. Hasła powinny być okresowo zmieniane (co 30-90 dni).Użytkownikowi systemu nie wolno udostępniać swojego identyfikatora ani hasła innym osobom.

4. Redundancja sprzętowa i programowa.

Dla zapewnienia wysokiej niezawodności systemu ASI opracowuje i wprowadza procedury awaryjne (np. w wypadku uszkodzenia głównego serwera/komputera/urządzenia gromadzącego dane).Należy rygorystycznie przestrzegać wymogu przechowywania nośników zawierających awaryjne kopie danych i systemów w pomieszczeniach innych niż pomieszczenia, w których przechowywane są dane przeznaczone do bieżącego użytku. Jednocześnie dane te muszą być odpowiednio zabezpieczone fizycznie (najlepiej ognioodporny sejf w zabezpieczonym pomieszczeniu).

5. Zapewnienie stałego zasilania energią.

Ciągłe zasilanie serwerom zapewniać powinno stosowanie zasilaczy awaryjnych UPS. W przypadku stacji roboczych, UPS stosuje się w zależności od potrzeb i możliwości finansowych.

6. Procedury awaryjne i procedury na wypadek klęsk żywiołowych i ewakuacji.

Zapewnieniu ciągłej dostępności informacji służą procedury postępowania w przypadku wydarzeń losowych (np. awaria serwera, zalanie pomieszczenia, pożar, itp.). Procedury takie powinny obejmować uruchomienie systemu w minimalnej konfiguracji udostępniającej zasoby systemu. Komputery przewidywane na awaryjne serwery powinny stać w pomieszczeniach innych niż serwery na bieżąco eksploatowane. W przypadku ewakuacji należy w pierwszej kolejności zapewnić bezpieczeństwo danym.

7. Procedury tworzenia kopii zapasowych, ich przechowywania i ochrony.

Dla systemów finansowych kopie bezpieczeństwa wykonuje się dwa do czterech razy w miesiącu. Dla pozostałych danych o częstotliwości składowania decyduje ASI, nie rzadziej jednak niż raz w miesiącu. Kopie zapasowe przechowuje się w ognioodpornym sejfie lub szafie umieszczonej w pomieszczeniu innym, niż dane przetwarzane na bieżąco. Pomieszczeniem tym jest Archiwum usytuowane na piętrze budynku. Kopie awaryjne podlegają takiej samej ochronie jak serwery zawierające dane na bieżąco przetwarzane. Pomieszczenie, w którym są przechowywane kopie bezpieczeństwa powinny być objęte, w zależności od potrzeb i możliwości finansowych, elektronicznym systemem wykrywania pożaru.

8. Profilaktyka antywirusowa.

Wszystkie serwery a także wszystkie stacje robocze uczestniczące w przetwarzaniu danych osobowych muszą posiadać zainstalowany i aktualny system antywirusowy sprawdzający w trybie rzeczywistym wszystkie pliki zapisywane i odczytywane, a także monitorować połączenia internetowe oraz pocztę elektroniczną. Baza definicji wirusów powinna być aktualizowana możliwie jak najczęściej. Zabronione jest blokowanie pracy tego programu. Dla zapewnienia ochrony przed wirusami serwer oraz stacje robocze powinny być okresowo (nie rzadziej niż co dwa miesiące) objęte pełnym testem antywirusowym.

9. Monitorowanie systemu ochrony i prowadzenie dziennika zdarzeń.

Systemy operacyjne komputerów powinny prowadzić dzienniki zdarzeń zawierające opis wszystkich ważniejszych czynności wykonywanych przesz użytkowników. Należy określić zdarzenia, które powinny być rejestrowane, jak również tryb postępowania z tymi dziennikami (co rejestrować, w jaki sposób i jak długo składować).

10. Przeciwdziałanie nowym technikom łamania zabezpieczeń oraz eliminacja luk wykrytych w zabezpieczeniach systemów.

W związku z dynamicznym rozwojem technik służących do atakowania systemów informatycznych, ASI powinien na bieżąco śledzić informacje na temat wykrytych luk i wprowadzać zalecane zabezpieczenia (jak łaty dla systemów operacyjnych i aktualizacja oprogramowania).

11. Procedury postępowania z nośnikami informacji i wydrukami (wytwarzanie, rejestrowanie, kasowanie, niszczenie)

Dla zachowania wysokiego poziomu bezpieczeństwa informacji w systemie informatycznym określa się procedury postępowania z nośnikami (dyskietki, płyty CD/DVD, nośniki papierowe) zawierającymi informacje od chwili wytworzenia do chwili skasowania lub zniszczenia. Dla zapewnienie szczelności systemu powinno się dążyć do pełnego ewidencjonowania i opisu nośników zawierających newralgiczne dane.

12. Testy okresowe systemu ochrony

System ochrony powinien być w sposób ciągły nadzorowany i możliwie często aktualizowany. Kontrole i testy powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników. Zapisy logów systemowych powinny być przeglądane codziennie oraz każdorazowo po wykryciu naruszanie zasad bezpieczeństwa.

13. Zabezpieczenia medium transmisyjnego

Połączenia z sieci wewnętrznej do sieci zewnętrznej (Internet) mogą być wykonywane tylko za pośrednictwem routerów wyposażonych w odpowiednio skonfigurowaną zaporę firewall. Zasada konfigurowania zapory ogniowej powinna uwzględniać blokowanie wszelkich usług nie będących niezbędnymi do prawidłowego funkcjonowania UG Giby. Powinny być także blokowane wszelkie połączenia przychodzące z sieci zewnętrznej, które nie są powiązane z zapoczątkowanymi połączeniami wychodzącymi z sieci wewnętrznej (established/related).

14. Konserwacja i naprawy sprzętu i oprogramowania

Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po uzyskaniu zgody ABI

Załącznik Nr 2 do Zarządzenia Nr 21/11

Wójta Gminy Giby

z dnia 8 kwietnia 2011 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Gibach.

§ 1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy w Gibach określa:

1. sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,

2. sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,

3. procedury rozpoczynania i kończenia pracy,

4. metodę i częstotliwość tworzenia kopii awaryjnych,

5. metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,

6. sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,

7. sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych, sposób postępowania w zakresie komunikacji w sieci komputerowej.

§ 2. Podstawowe zasady przetwarzania danych osobowych;

1. Przetwarzanie danych osobowych może odbywać się zgodnie z obowiązującą ustawą o ochronie danych osobowych oraz wykonawczymi dokumentami normatywnymi.

2. Osobą odpowiedzialną za bezpieczeństwo danych w systemach informatycznych przetwarzających dane osobowe jest ABI.

3. Przetwarzanie danych osobowych jest możliwe tylko przez uprawnione osoby w wyznaczonym przez ADO obszarze (budynku, pomieszczeniu lub części pomieszczenia) podlegającym szczególnej ochronie bezpieczeństwa.

4. Udostępnianie danych osobowych może odbywać się tylko za zgodą ADO na wniosek przygotowany w oparciu o art. 29 ust. 1 ustawy o ochronie danych osobowych oraz wg wzoru określonego w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r. (Dz. U. Nr 80, poz. 522), chyba, że przepis innej ustawy stanowi inaczej.

5. Zgodnie z ustawą o ochronie danych osobowych, udostępniane dane mogą być wykorzystane wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione (art. 29 ust 4) a przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt. 4).

§ 3. 1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej "systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez ABI.

2. Rejestracja, o której mowa w ust. 1, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§ 4. 1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zwierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

3. Zmiana hasła następuje w okresach od 30 do 90 dni.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 5. 1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje ABI.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter tymczasowy lub stały.

3. Wyrejestrowanie następuje poprzez:

1. zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

2. usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

1. nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,

2. zawieszenie w pełnieniu obowiązków służbowych,

3. zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 6. Rozpoczęcie pracy w systemie odbywa się poprzez:

1. przygotowanie stanowiska pracy,

2. włączenie stacji roboczej,

3. połączenie z serwerem,

4. wprowadzenie swojego identyfikatora i hasła.

§ 7. Zakończenie pracy w systemie odbywa się poprzez:

1. zamknięcie aplikacji,

2. odłączenie od zasobów systemowych,

3. zamknięcie połączenia z serwerem,

4. zamknięcie systemu operacyjnego,

5. wyłączenie stacji roboczej.

§ 8. Zabrania się użytkownikom:

1. udostępniania stacji roboczej osobom niezarejestrowanym w systemie w trybie określonym w §1 ust. 2,

2. udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z ABI,

3. użytkowania nielicencjonowanego oprogramowania,

4. samodzielnego instalowania oprogramowania,

5. używania w stacjach roboczych własnych, niezatwierdzonych przez ADO (dyskietki, płyty CD/DVD, urządzenia masowe USB, itp.),

6. używania stacji roboczych do czynności innych niż służbowe.

§ 9. 1. Każdy przypadek naruszenia ochrony danych osobowych podlega zgłoszeniu do ABI, a w szczególności:

1. naruszenie bezpieczeństwa systemu informatycznego,

2. stwierdzenie objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci), które mogą wskazywać na naruszenie bezpieczeństwa.

2. ABI zgłasza się w szczególności przypadki:

1. użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,

2. usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,

3. usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów lub rekordów,

4. przebywania osób nieupoważnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody ADO, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

5. udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

6. niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,

7. przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,

8. przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust. 1, spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem ABI jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. ASI w porozumieniu z ABI ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 10. 1. Za sporządzanie kopii bezpieczeństwa informacji znajdujących się na serwerach odpowiada ASI. Wykonywanie kopii bezpieczeństwa danych znajdujących się na stacjach roboczych należy do użytkowników. Dopuszcza się wykonywanie kopii bezpieczeństwa przy wykorzystaniu dyskietek, płyt CD/DVD, streamerów, dysków twardych i innych urządzeń zapewniających odpowiednią trwałość przechowywanych danych. Przy większych zbiorach i braku w stacji roboczej odpowiedniego mechanizmu składowania należy kontaktować się z ASI i z nim ustalić sposób składowania. Zaleca się zapisywanie istotnych zbiorów danych na udostępnionych przez administratora dyskach sieciowych.

2. Kopie bezpieczeństwa tworzy się z następującą częstotliwością:

1. kopie systemu finansowo-księgowego - dwa do czterech razy w miesiącu,

2. kopie systemu podatkowego – raz w miesiącu,

3. kopie systemu ewidencji ludności - raz w tygodniu,

4. kopie systemu kadrowo-płacowego - raz w tygodniu,

5. kopie systemu Płatnik - raz w tygodniu,

6. pozostałe - nie rzadziej niż raz na miesiąc.

3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytku.

4. ASI przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia ASI do ich zniszczenia.

§ 11. 1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, ASI nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach jak również w serwerach.

4. Za sprawdzenie obecności wirusów na stacjach roboczych odpowiedzialni są użytkownicy systemu. Sprawdzenie nie powinno być wykonywane rzadziej niż raz na dwa miesiące.

5. W przypadku pozytywnego wyniku testu (wykrycie wirusa), o którym mowa w ust. 4, użytkownik systemu zobowiązany jest niezwłocznie powiadomić o tym fakcie ASI i zaprzestać przetwarzania danych osobowych do czasu usunięcia problemu.

6. Do obowiązków ASI należy aktualizacja oprogramowania służącego do sprawdzania w systemie oraz na serwerach obecności wirusów komputerowych.

7. Obowiązek dbania o aktualizacje do najnowszej wersji bazy sygnatur wirusów na stacjach roboczych spoczywa na użytkownikach systemu.

8. W przypadku problemów z wykonaniem aktualizacji, o której mowa w ust. 7, użytkownik systemu zobowiązany jest do natychmiastowego powiadomienia o tym fakcie ASI.

§ 12. 1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilanie energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwerów oraz stacji roboczych w zasilacze awaryjne (UPS).

§ 13. 1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać:

1. do naprawy,

2. podmiotowi nieuprawnionemu do otrzymania tych danych,

3. do likwidacji dopiero po uprzednim uzyskaniu zgody ABI.

2. Urządzenia, o których mowa w ust. 1, przed ich przekazaniem pozbawia się zapisu danych osobowych.

3. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 14. 1. Przeglądu i konserwacji systemu dokonuje ASI doraźnie.

2. Przeglądu plików zawierających raport dotyczący działalności aplikacji bądź systemu (log systemowy) ASI dokonuje nie rzadziej niż raz na dwa tygodnie.

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik systemu przy współudziale ASI nie rzadziej niż raz na dwa tygodnie.

§ 15. 1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe ASI zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępniania zasobów na serwerze, administrator systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 16. 1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być wykonane w sposób umożliwiający dostęp tylko użytkownikom uprawnionym i wyznaczonym przez ASI, przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, ASI wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 17. Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych z uwzględnieniem przepisów prawnych uwzględniających wysyłanie tych danych.

§ 18. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§ 19. 1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają funkcję eksploatacji ekranu.

§ 20. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie ABI o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. ABI może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

§ 21. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§ 22. 1. Wszystkie komputery (serwery i stacje robocze) Urzędu Gminy biorące udział w przetwarzaniu danych osobowych są wyposażone w oprogramowanie antywirusowe. Zabrania się wyłączania tego oprogramowania. Dane zawarte na nośnikach zewnętrznych (np. dyskietki) muszą być sprawdzone przez program antywirusowy przed wprowadzeniem ich do systemu. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z ASI.

2. Użytkownicy stacji roboczych nie mają prawa dokonywać samodzielnie jakichkolwiek instalacji oprogramowania zarówno na stacjach roboczych, jak i na serwerach sieci. Za instalację i konfigurację oprogramowania odpowiadają wyznaczone osoby zajmujące się administracją. ASI i ABI są odpowiedzialni za instalację uaktualnień oprogramowania.

3. ASI przygotowuje a ADO zatwierdza listę oprogramowania dopuszczoną do użytkowania na stacjach roboczych w zależności od typu prac na nich wykonywanych.

4. Zabrania się wszelkich prac z wykorzystaniem oprogramowania, na które użytkownik nie ma ważnej licencji (zakaz nie dotyczy programów, na użytkowanie których licencja nie jest wymagana) lub niewiadomego pochodzenia.

5. Przy wprowadzaniu do systemu nowych programów lub danych zawsze należy kierować się zasadą ograniczonego zaufania.

§ 23. Wykonywanie prac pozasłużbowych na komputerach dopuszcza się w wyjątkowych przypadkach - za zgodą przełożonych.

§ 24. Zabrania się pozostawiania sprzętu komputerowego niezabezpieczonego przed dostępem osób nieuprawnionych, bez nadzoru osoby odpowiedzialnej za jego użytkowanie. Zalecane jest stosowanie wygaszaczy ekranu zabezpieczonych hasłem.

§ 25. 1. Użytkownik systemu sporządzający wydruki, które zwierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu na podstawie indywidualnego zakresu czynności.

2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

Załącznik Nr 3 do Zarządzenia Nr 21/11

Wójta Gminy Giby

z dnia 8 kwietnia 2011 r.

Instrukcja
postępowania w sytuacji naruszenia zasad ochrony danych osobowych
w Urzędzie Gminy w Gibach.

§ 1. Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych wykorzystywanych w Urzędzie Gminy w Gibach.

§ 2. Instrukcja określa tryb postępowania w przypadku gdy:

1. stwierdzono naruszenie zabezpieczeń systemu informatycznego,

2. stan urządzeń, zawartość zbiorów danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość transmisji w sieci mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 3. Każda osoba zatrudniona w Urzędzie Gminy w Gibach, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych w systemach informatycznych Urzędu Gminy, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych, ABI, ASI lub ADO.

§ 4. Każde domniemanie, przesłanki, fakt wskazujący na naruszenie zasad ochrony danych osobowych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, w tym;

1. stan urządzeń systemu zabezpieczeń obiektu,

2. stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,

3. zawartość zbioru danych,

4. ujawnione metody pracy,

5. sposób działania programu,

6. jakość komunikacji w sieci telekomunikacyjnej,

7. przebywanie osób nieuprawnionych wewnątrz obszaru przetwarzania danych osobowych,

8. inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego w tym obecność wirusów, stanowi dla każdej osoby uprawnionej do przetwarzania danych osobowych podstawę do natychmiastowego reagowania.

§ 5. Sposób postępowania:

1. O każdej sytuacji odbiegającej od norm, a w szczególności o przesłankach naruszenia zasad ochrony danych osobowych w systemie informatycznym, opisanych w §4, należy natychmiast informować ABI lub osobę przez niego upoważnioną.

2. Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo zobowiązana jest do możliwie pełnego udokumentowania zdarzenia celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.

3. Stwierdzone przez ABI naruszenie zasad ochrony danych osobowych wymaga powiadomienia ADO oraz natychmiastowej reakcji poprzez:

1) usunięcie uchybień,

2) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,

3) wstrzymanie przekazywania i udostępniania danych.

4. W sytuacji naruszenia zasad ochrony danych osobowych, po wcześniejszym wykonaniu czynności opisanych w pkt. 3 ABI niezwłocznie sporządza informację na piśmie przedstawiając ADO przyczyny, skutki i poczynione działania zabezpieczające i prewencyjne.

§ 6. ABI lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:

1. Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby nieuprawnionej, zminimalizować szkody i zabezpieczyć przed usunięciem śladów jej ingerencji poprzez:

1) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do baz danych osobie nieuprawnionej,

2) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczeń baz danych zawierających dane osobowe,

3) zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

2. Zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu.

3. Na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem.

4. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieuprawnionej.

5. Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie.

6. ABI lub inna upoważniona przez niego osoba powinna sprawdzić:

1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

2) zawartość zbioru danych osobowych,

3) sposób działania programu,

4) jakość komunikacji w sieci teletransmisyjnej,

5) wykluczyć możliwość obecności wirusów komputerowych,

6) po dokonaniu powyższych czynności ABI winien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującą identyfikację rodzaju zaistniałego zdarzenia, metody dostępu do danych osoby nieuprawnionej, skali zniszczeń.

7. Niezwłocznie należy przywrócić normalny stan działania systemu, przy czym, jeżeli nastąpiło uszkodzenie baz danych, niezbędne jest jej odtworzenie z ostatniej kopii bezpieczeństwa z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osoby niepowołane.

8. Po przywróceniu prawidłowego stanu baz danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości,

9. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych osobowych.

10. Jeżeli przyczyną było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenie antywirusowe.

11. Jeżeli przyczyną było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje regulowane ustawą.

12. Jeżeli przyczyną było włamanie w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony baz danych.

13. Jeżeli przyczyną zdarzenia był zły stan urządzeń lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe.

§ 7. ABI przedstawi szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz w uzgodnionym z ADO terminie od daty zaistnienia zdarzenia przekaże go archiwum Urzędu Gminy.

§ 8. Instrukcja wchodzi w życie z dniem podpisania.

Załącznik Nr 4 do Zarządzenia Nr 21/11
Wójta Gminy Giby
z dnia 8 kwietnia 2011 r.

Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

Dane osobowe przetwarzane są w budynku Urzędu Gminy w Gibach, Giby 74a, 16-506 Giby.

L.p.	**Nr pokoju (kondygnacja), w którym przetwarzane są dane osobowe.**
1.	Pokój nr 1 (Piętro)
2.	Pokój nr 2 (Piętro)
3.	Pokój nr 3 (Piętro)
4.	Pokój nr 4 (Piętro)
5.	Pokój nr 5 (Piętro)
6.	Pokój nr 6 (Piętro)
7.	Pokój nr 7 (Piętro)
8.	Pokój nr 8 (Piętro)
9.	Pokój nr 1 (Parter)
10.	Pokój nr 3 (Parter)
11.	Pokój nr 2 - Serwerownia (Suterena)

Załącznik Nr 5 do Zarządzenia Nr 21/11

Wójta Gminy Giby

z dnia 8 kwietnia 2011 r.

O Ś W I A D C Z E N I E

Ja, niżej podpisana(y), oświadczam, że zapoznała(e)m się z przepisami dotyczącymi przetwarzania i ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

2. Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

Jednocześnie oświadczam, że:

a) zachowam w tajemnicy wszelkie informacje dotyczące bezpieczeństwa danych osobowych oraz sposobów ich zabezpieczenia;

b) zapewnię bezpieczeństwo i ochronę danym osobowym przetwarzanym w wyniku realizacji umowy (porozumienia), a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem;

c) natychmiast zgłoszę swoim przełożonym i Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy w Gibach (ABI), stwierdzenie próby lub faktu naruszenia ochrony danych orazzagrożenia ich bezpieczeństwa w systemach informatycznych.

....…….....

(podpis osoby ubiegającej się o upoważnienie)

Giby, dnia.....

Oświadczenie wypełnia osoba, która wykonując swoje obowiązki posiada lub może posiadać dostęp do danych osobowych przetwarzanych w Urzędzie Gminy w Gibach. Składanie oświadczenia jest zgodne z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

Załącznik Nr 6 do Zarządzenia Nr 21/11
Wójta Gminy Giby
z dnia 8 kwietnia 2011 r.

Wniosek o wydanie upoważnienia do przetwarzania danych osobowych.

…..... Giby, dn. .....

(nazwa komórki organizacyjnej)

Administrator Danych Osobowych
Wójt Gminy Giby
Giby 74A
16-506 Giby

W N I O S E K

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

w n i o s k u j ę o nadanie/ zmianę/ pozbawienie/ *

Pani /Pan/*.....
upoważnienia do przetwarzania danych osobowych w Urzędzie Gminy w Gibach z powodu:
/przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy, zmiany uprawnień, lub innego /jakiego/, nr umowy o dzieło lub zlecenie/data zawarcia/czas trwania/ ***** :
.....….....

Upoważnienie wydaje się na okres: /stały/czasowy - **do kiedy** /*.....

1. Zakres przetwarzania danych osobowych:
a) zbiory własnej komórki organizacyjnej ……..…….....
……..……..
……..……..
b) zbiory innych komórek/**……...…….....
……..……..
……..……..
2. Uprawnienia: użytkownika /użytkownika uprzywilejowanego/ ASI/* z tytułu zajmowanego stanowiska /jakiego/:
.....
3. Sposób przetwarzania danych osobowych: papierowy/informatyczny/*
4. Obszar przetwarzania /adres / .....
danych osobowych /piętro, nr pokoju/ .....
5. Uprawnienia obejmują przetwarzanie danych sensytywnych /art. 27 Ustawy/:
/tak/nie/ *****
6. Dodatkowe informacje dotyczące wyrażenia zgody przez osoby administrujące zbiorami na

imienne rozszerzenie przetwarzania danych:

…….

……

(imię , nazwisko i stanowisko przełożonego)

/* niepotrzebne proszę skreślić ;

/ wymaga zgody Administrującego danym zbiorem.**

[Dot. osób niebędących pracownikami Urzędu]

.....

(imię i nazwisko)

.....

(nazwa podmiotu - firmy)

Załącznik Nr 7 do Zarządzenia Nr 21/11

Wójta Gminy Giby

z dnia 8 kwietnia 2011 r.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY GIBY

(art. 39 ustawy o ochronie danych osobowych)

L.p.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia (zawartość zbioru danych)	Identyfikator

.