ZARZĄDZENIE NR 13/2018
WÓJTA GMINY MIEDŹNO

z dnia 29 stycznia 2018 r.

w sprawie Polityki Bezpieczeństwa

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), § 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) oraz art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875 z późn. zm.)

zarządza się, co następuje:

POLITYKA BEZPIECZEŃSTWA

§ 1. 1. Ilekroć w zarządzeniu jest mowa o:

1) Polityce bezpieczeństwa - rozumie się przez to Politykę bezpieczeństwa obowiązującą w Urzędzie Gminy Miedźno, opracowaną 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. Nr 100, poz. 1024);

2) 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;

3) 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;

4) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

5) zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

6) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

7) administratorze danych - rozumie się przez to Wójta Gminy Miedźno;

8) administratorze bezpieczeństwa informacji – rozumie się przez to osobę powołaną przez Administratora Danych której zadania określone są w art. 36a ust. 2 i 4 chyba, że Administrator Danych sam wykonuje te czynności;

9) urzędzie – rozumie się przez to Urząd Gminy Miedźno;

10) ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922).

§ 2. 1. Polityka bezpieczeństwa 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 manualnych oraz w systemach informatycznych.

4. Polityka bezpieczeństwa określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.

5. Polityka bezpieczeństwa dotyczy wszystkich danych osobowych przetwarzanych w urzędzie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

6. Polityka bezpieczeństwa ma zastosowanie wobec wszystkich komórek organizacyjnych w tym referatów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

§ 3. 1. Celem Polityki bezpieczeństwa jest przetwarzanie danych osobowych przetwarzanych w urzędzie zgodnie z przepisami oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

2. Cele Polityki bezpieczeństwa realizowane są poprzez zapewnienie danym osobowym następujących cech:

1) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;

2) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

3) rozliczalności - właściwości zapewniającej, że działania urzędu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

4) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

§ 4. 1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

§ 5. Dla skutecznej realizacji Polityki bezpieczeństwa Administrator Danych zapewnia:

1) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;

2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;

3) kontrolę i nadzór nad przetwarzaniem danych osobowych;

4) monitorowanie zastosowanych środków ochrony, co obejmuje w szczególności:

   a) działania użytkowników,

   b) naruszanie zasad dostępu do danych,

   c) zapewnienie integralności plików oraz ich ochronę przed atakami zewnętrznymi oraz wewnętrznymi;

5) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;

6) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

§ 6. 1. Administrator Danych zapewnienia bezpieczeństwo przetwarzanych danych osobowych w szczególności poprzez:

1) uwzględnianie faktu nieustannego powstawania nowych i zmienia się rodzaju i charakteru istniejących zagrożeń;

2) wspieranie w urzędzie przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych;

3) uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w Polityce bezpieczeństwa.

2. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy oraz innych przepisów mających zastosowanie przy przetwarzaniu danych osobowych.

§ 7. Środki ochrony dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują w szczególności:

1) środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);

2) środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);

3) środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym).

§ 8. Środki ochrony fizycznej pomieszczeń, obejmują w szczególności:

1) drzwi zwykłe zamykane na 2 klucze oraz zamki szyfrowe;

2) okna zabezpieczone szybami antywłamaniowymi;

3) dostęp tylko w obecności osób upoważnionych;

4) przechowywanie danych w pomieszczeniach zabezpieczonych przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolno stojącej gaśnicy;

5) zawierających dane osobowe po ustaniu przydatności niszczeniem w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 9. Środki techniczne obejmują w szczególności:

1) urządzenia chroniące przed skutkami awarii zasilania (np. ups);

2) zabezpieczenie za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

3) zmianę haseł nie rzadziej niż co 30 dni;

4) rejestrację dostępu do systemów informatycznych;

5) zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony;

6) system Firewall;

7) rejestrację zmian wykonanych na danych w systemach informatycznych;

8) określenia praw dostępu do zakresu w ramach przetwarzanych zbiorów;

9) wygaszacze ekranów;

10) automatyczną blokadę dostępu do systemu w przypadku dłuższej nieaktywności pracy użytkownika:

11) zastosowanie mechanizmu wymuszającego okresową zmianę haseł dostępu do bazy danych osobowych;

12) systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;

13) stosowanie indywidualnych haseł logowania do poszczególnych programów;

14) zastosowanie właściwej budowy hasła.

§ 10. 1. Środki organizacyjne obejmują:

1) wdrożenie Instrukcji Zarzadzania Systemem Informatycznym;

2) dostęp do danych wyłącznie przez osoby upoważnione i zapoznane z przepisami dotyczącymi ochrony danych osobowych;

3) przeszkolenie Administratora Danych Osobowych;

4) przeszkolenie osób zatrudnionych przy przetwarzaniu danych osobowych;

5) osoby upoważnione zostały zobowiązane do zachowania tajemnicy dotyczącej danych osobowych;

6) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

7) ustawienie monitorów komputerów, na których przetwarzane są dane osobowe w sposób uniemożliwiający wgląd osobom postronnym;

8) powołanie Administratora Bezpieczeństwa Informacji.

§ 11. 1. Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ustawie.

2. Administrator danych zapewnia środki i organizacyjną odrębność Administratorowi Bezpieczeństwa Informacji, niezbędne do należytego wykonywania przez niego zadań wynikających z przepisów ustawy o ochronie danych osobowych oraz Polityki bezpieczeństwa.

3. Niezwłocznie po wyznaczeniu Administrator Bezpieczeństwa Informacji składa Administratorowi Danych oświadczenie o przyjęciu obowiązków i spełnianiu wymagań określnych w przepisach prawa, niezbędnych do pełnienia tej funkcji. Wzór oświadczenia stanowi załącznik nr 1 do zarządzenia.

§ 12. 1. Do zadań Administratora Bezpieczeństwa Informacji należy:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 zgodnie z zapisami rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. poz. 745);

3) opracowywanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych;

4) nadzorowanie przestrzegania w urzędzie przepisów Instrukcji Zarządzania Systemem Informatycznym;

5) prowadzenie wszelkiej dokumentacji opisującą sposób przetwarzania danych w podmiocie, a w szczególności:

   a) wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, zgodnie ze wzorem stanowiącym załącznik nr 2 do zarządzenia,

   b) wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zgodnie ze wzorem stanowiącym załącznik nr 3 do zarządzenia,

   c) opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, zgodnie ze wzorem stanowiącym załącznik nr 4 do zarządzenia,

   d) rejestru osób przetwarzających dane w urzędzie posiadających upoważnienie, zgodnie ze wzorem stanowiącym załącznik nr 5 do zarządzenia,

   e) zestawienia danych osobowych, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, zgodnie ze wzorem stanowiącym załącznik nr 6 do zarządzenia,

   f) wykazu zastosowanych w Urzędzie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, zgodnie ze wzorem stanowiącym załącznik nr 7 do Zarządzenia;

6) sprawdzanie zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla administratora danych lub na wniosek GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. poz. 745);

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

8) przeprowadzanie wraz z wyznaczonymi Użytkownikami okresowej analizy ryzyka dla systemu i na jej podstawie przedstawianie Administratorowi Danych propozycji dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych;

9) określenia poziomu bezpieczeństwa systemu informatycznego.

§ 13. 1. W urzędzie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych.

2. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 14. 1. Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych.

2. Administrator Danych nadaje na wniosek Administratora Bezpieczeństwa Informacji uprawnienia pracownikom, którzy przetwarzają dane, poprzez podpisanie upoważnienia, którego wzór stanowi załącznik nr 8 do zarządzenia.

3. Administrator Bezpieczeństwa Informacji prowadzi dokumentację opisująca sposób przetwarzania danych w urzędzie.

§ 15. Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji określonych w art. 32 ust. 1 pkt 1-5 a ustawy.

§ 16. 1. Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w urzędzie.

2. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 17. Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 18. 1. Za niedopełnienie obowiązków wynikających z Polityki bezpieczeństwa pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

2. W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą.

3. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w Polityce bezpieczeństwa.

§ 19. W sprawach nieuregulowanych w Polityce Bezpieczeństwa mają zastosowanie odpowiednie przepisy 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).

§ 20. Zobowiązuje się wszystkich pracowników urzędu do zapoznania się z treścią Polityki bezpieczeństwa oraz przestrzegania zasad w niej zawartych.

§ 21. Wykonanie zarządzenia powierza się Sekretarzowi Gminy oraz Administratorowi Bezpieczeństwa Informacji.

§ 22. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Miedźno

Piotr Derejczyk

Załącznik Nr 1 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór oświadczenia Administratora Bezpieczeństwa Informacji

OŚWIADCZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

1. Oświadczam, że zapoznałem się z obowiązkami Administrator Bezpieczeństwa Informacji, oraz, że jako Administrator Bezpieczeństwa Informacji, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie Urzędzie Gminy Miedźno zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

2. Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko Administratora Bezpieczeństwa informacji tj.:

a) nie byłam/byłem karana/y za umyślne przestępstwo,

b) posiadam pełną zdolność do czynności prawnych oraz korzystam z pełni praw publicznych,

c) posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

.....

Administrator Bezpieczeństwa Informacji

Miedźno, ...

Załącznik Nr 2 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi

….....

Data i podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 3 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Uwagi**

….....

Data i podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 4 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Struktura zbiorów** *(np. imię i nazwisko, e-mail, telefon itd.)*	**Przepływ danych** *(np. wydruk danych z Internetu)*	**Uwagi**

….....

Data i podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 5 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór rejestru osób przetwarzających dane w Urzędzie Gminy Miedźno posiadających upoważnienie

REJESTR OSÓB PRZETWARZAJĄCYCH DANE W URZĘDZIE GMINY MIEDŹNO POSIADAJĄCYCH UPOWAŻNIENIE

Lp.	**Imię i nazwisko**	**Stanowisko służbowe**	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Wykaz zbiorów danych wynikających z upoważnienia**	**Identyfikator** *(Jeżeli dane są przetwarzane w systemie informatycznym)*

….....

Data i podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 6 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór zestawienia danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane

ZESTAWIENIE DANYCH OSOBOWYCH Z INFORMACJĄ KIEDY I PRZEZ KOGO ZOSTAŁY DO ZBIORU WPROWADZONE ORAZ KOMU SĄ PRZEKAZYWANE

Lp.	Rodzaj udostępnionych danych osobowych	Data wprowadzenia danych do zbioru	Data przekazania danych osobowych	Imię i nazwisko osoby która otrzymała dane	Cel przekazania danych osobowych

….....

Data i podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 7 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór wykazu zastosowanych w Urzędzie Gminy Miedźno środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

WYKAZ ZASTOSOWANYCH W URZĘDZIE GMINY MIEDŹNO ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Lp.	**Nazwa**	**Rodzaj** *(środek ochrony fizycznej/ technicznej/ organizacyjnej)*	**Miejsce wprowadzenia/ zastosowania**	**Data wprowadzenia/ zastosowania**	**Uwagi**

….....

Data i podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 8 do Zarządzenia Nr 13/2018

Wójta Gminy Miedźno

z dnia 29 stycznia 2018 r.

Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Wójt Gminy jako Administrator Danych, dnia ..... nadaje upoważnienie do przetwarzania danych osobowych w podmiocie Urzędzie Gminy Miedźno dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

….....

….....

….....

Upoważnienie nadaje się do dnia: na czas pełnienia obowiązków służbowych

Administrator Danych

….....

Podpis

OŚWIADCZENIE UPOWAŻNIONEGO

Ja, niżej podpisany zobowiązuje się do przestrzegania zasad obowiązujących w Urzędzie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania przepisów **Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.)** Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w Urzędzie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych **(Dz. U. z 2016 r. poz. 922 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).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Użytkownik

….....

Podpis