

**ZARZĄDZENIE NR 81.2015
WÓJTA GMINY MIŁKI
z dnia 30 lipca 2015 r.**

w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcja zarządzania systemem informatycznym w Urzędzie Gminy Miłki

Na podstawie art. § 3 i § 4 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. 36 ust. 2 i art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 z późn. zm.)¹ zarządzam, co następuje:

§ 1

1. Dla zapewnienia ochrony przetwarzania danych osobowych wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Miłki” stanowiącą załącznik Nr 1 do niniejszego zarządzenia.
2. Wdrażam „Instrukcję zarządzania systemem informatycznym” stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Miłki i Instrukcja zarządzania systemem informatycznym ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym.

§ 3

Zobowiązuję Administratora Systemu Informatycznego do zapoznania pracowników z treścią załączników do niniejszego zarządzenia.

§ 4

Traci moc zarządzenie Nr 5/2012 Wójta Gminy Miłki z dnia 25 stycznia 2012 roku.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJTA GMINY MIŁKI

Barbara Małgorzata Mazurczyk

¹ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2014 r. poz. 1662 oraz z 2015 r. poz. 1309.

POLITYKA BEZPIECZEŃSTWA

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Gminy Miłki, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekoć 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 jakiegokolwiek 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, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. 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,
7. 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.
8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3

Administrator Danych w podmiocie Urząd Gminy Miłki 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. Upoważnienie dla Administratora Bezpieczeństwa Informacji określa załącznik do „Polityki Bezpieczeństwa” nr 1.

§ 4

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

§ 5

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

§ 6

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

§ 7

Administradora Bezpieczeństwa Informacji dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych. 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. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi załącznik nr 5 do „Polityki Bezpieczeństwa”. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – załącznik nr 6 do „Polityki Bezpieczeństwa”
2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – załącznik nr 7 do „Polityki Bezpieczeństwa”
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - załącznik nr 8 do „Polityki Bezpieczeństwa”

§ 9

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

§ 10

Administrator Bezpieczeństwa Informacji 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.

§ 11

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

§ 12

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.

Deklaracja intencji, cele i zakres polityki bezpieczeństwa

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym referatów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
5. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.
7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
 - a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
 - b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
 - c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
 - d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.
8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
 - a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
 - b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
 - c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
 - d) monitorowanie zastosowanych środków ochrony;
 - e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
 - f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.
9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie dokumenty składające się na Polityki Bezpieczeństwa i zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych:

- a) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
- b) 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);
- c) innymi przepisami mającymi zastosowania przy przetwarzaniu danych osobowych.

Podpis Administratora Danych Osobowych

WÓJT GMINY MAŁKI

.....
Barbara Małgorzata Nizkarczyk

Podpis

Podpis Administratora Bezpieczeństwa Informacji

ADMINISTRATOR
BEZPIECZEŃSTWA INFORMACJI

Susłyń
.....
Agnieszka Grajewska-Susłyń

Podpis

.....
miejsowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

Na podstawie § 2 Polityki Bezpieczeństwa z dnia 30 lipca zgodnie z założeniami 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 art. 36a.1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014 r. poz. 1182, 1662) Barbara Małgorzata Mazurczyk-Wójt Gminy Miłki, jako Administrator Danych Osobowych w Urzędzie Gminy Miłki

upoważniam

Pana/Panią **do pełnienia funkcji**
Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Miłki

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez Administrator Danych.

Administrator Bezpieczeństwa Informacji jest zobowiązany 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, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Bezpieczeństwa Informacji jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie, a w szczególności: zgodnie z § 4. „Polityki Bezpieczeństwa” wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa” nr 2, zgodnie z § 5. „Polityki Bezpieczeństwa” wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa” nr 3, zgodnie z § 6. „Polityki Bezpieczeństwa” opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa” nr 4, zgodnie z § 8. „Polityki Bezpieczeństwa” ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa”, zestawienie danych osobowych - kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – załącznik nr 7 do „Polityki Bezpieczeństwa”.

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w Urzędzie Gminy Miłki zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji

Administrator Danych

.....
podpis

.....
podpis

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

Lp.	Dokładny adres <i>(np. adres siedziby firmy gdzie przetwarzane są dane)</i>	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi

Data i podpis Administratora 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 Danych

.....

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.)	Przeptyw danych (np. wydruk danych z internetu)	Uwagi

Data i podpis Administratora Danych

.....

Upoważnienie do przetwarzania danych osobowych

Wójt Gminy Miłki jako Administrator Danych w Urzędzie Gminy Miłki
dnia nadaje upoważnienie do przetwarzania danych osobowych
w Urzędzie Gminy Miłki 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

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie 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 2014 r. poz. 1182,1662) 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 ze zm.).

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.

Administrator Danych

.....

Podpis

Użytkownik

.....

Podpis

Ewidencja osób przetwarzających dane w podmiocie 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 Danych

.....

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. ABI wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.
3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI.
4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
5. Środki ochrony, zastosowane przez ABI dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
 - środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
 - środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS) ;
 - środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym) ;
6. Zastosowane środki ochrony fizycznej pomieszczeń:

7. Zastosowane środki techniczne obejmują:

8. Zastosowane środki organizacyjne obejmują:

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych. W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogą ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

Data i podpis Administratora Danych

.....

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§ 1

Za przestrzeganie zapisów „instrukcji” w Urzędzie Gminy Miłki odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa” wyznaczony Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego.

Ilekcioć w „instrukcji” jest mowa o:

- 1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
- 2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą”;
- 3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.);
- 6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
- 7) teletransmisji — rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
- 8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- 11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§2

W związku z tym, że w Urzędzie Gminy Miłki przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim, a w związku z tym wprowadza się poniższe postanowienia:

1. Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

2. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby: w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
4. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
 - 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego
 - a) poprzez zainstalowanie programu antywirusowego
 - b) poprzez zainstalowanie firewall (zapora sieciowa).
 - c) poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.
 - 2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień
8. Kopie zapasowe:
 - 1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym zaopatrzonym w system alarmowy
 - 2) usuwa się niezwłocznie po ustaniu ich użyteczności.
9. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.
10. Komputer przenośny może być wynoszony poza Urząd tylko za zgodą Administratora Systemu Informatycznego.
11. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
 - 1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
 - 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
 - 3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
 - 1) daty pierwszego wprowadzenia danych do systemu;
 - 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
 - 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
 - 4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
 - 5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych Administrator Bezpieczeństwa Informacji ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez Administratora Bezpieczeństwa Informacji uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7

W sprawach nieuregulowanych w niniejszej „instrukcji” mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz 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

.....
WÓJT GMINY MIŁKI

Podpis Administratora Danych Osobowych

ADMINISTRATOR
BEZPIECZEŃSTWA INFORMACJI

.....
Sedyra

Podpis Administratora Bezpieczeństwa Informacji

