Z a r z ą d z e n i e Nr 28/2018
Wójta Gminy Grudusk
z dnia 25 maja 2018r.

w sprawie wprowadzenia i wdrożenia do stosowania Polityki Bezpieczeństwa i Instrukcji zarzadzania systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Grudusk.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r., poz. 994 , ze zm.; Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z prztewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych) oraz § 3 ust.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) zarządzam co następuje:

§ 1

W celu zapewnienia należytego bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Grudusk w systemach informatycznych, wprowadza się:

1. Politykę Bezpieczeństwa wg załącznika Nr 1 do niniejszego zarządzenia.
2. Instrukcję Zarzadzania Systemem Informatycznym wg załącznika Nr 2 do niniejszego zarządzenia.

§ 2

Zobowiązuję pracowników Urzędu Gminy Grudusk do stosowania zasad określonych w w dokumentach wskazanych w § 1.

§ 3

Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 4

Traci moc zarządzenie Nr 28/2015 Wójta Gminy Grudusk z dnia 30 czerwca 2015 roku w sprawie wprowadzenia i wdrożenia do stosowania Polityki Bezpieczeństwa i instrukcji zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Grudusk.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Jacek Ogłęcki

Zał. Nr 1

POLITYKA BEZPIECZEŃSTWA

wraz z załącznikami:

1. Wykaz budynków, pomieszczeń – Zał. Nr 1
2. Rejestr czynności przetwarzania danych osobowych-wzór- Zał. nr 2
3. Rejestr kategorii czynności przetwarzania- wzór – Zał. Nr 3
4. Oświadczenie o poufności-wzór – Zał. Nr 4
5. Upoważnienie do przetwarzania danych osobowych – wzór- Zał. Nr 5
6. Ewidencja osób przetwarzających dane osobowe posiadających upoważnienie – Zał. Nr 6
7. Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – Zał. Nr 7
8. Określenie środków technicznych i organizacyjnych – Zał. Nr 8

§ 1.

„Polityka Bezpieczeństwa" w zakresie ochrony danych osobowych w Urzędzie Gminy Grudusk , 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

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych,
7. inspektorze ochrony danych – rozumie się przez to osobę wyznaczoną przez Administratora Danych zgodnie z art. 37 Rozporządzenia 2016/679 RODO, 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 Urząd Gminy Grudusk.

§ 3.

Administrator Danych w Urzędzie Gminy Grudusk wyznacza **Inspektora Ochrony Danych** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 10 maja 2018 roku o ochronie danych osobowych oraz Rozporządzenia Rady UE 2016/679 RODO.

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 1.**

§ 5.

Inspektor Ochrony Danych 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. Zadania Inspektora Ochrony Danych zostały zawarte w art 39 Rozporządzenia 2016/679.

§ 6.

Inspektor Ochrony Danych prowadzi rejestr czynności przetwarzania danych osobowych o którym mowa w art 30 ust.1. Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z prztewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych), który stanowi **załącznik nr 2 do „Polityki Bezpieczeństwa".**

§ 7.

inspektor Ochrony Danych prowadzi rejestr kategorii czynności przetwarzania danych osobowych o którym mowa w art 30 ust .2. Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z prztewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych), który stanowi **załącznik nr 3 do „Polityki Bezpieczeństwa".**

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych**.

Inspektor Ochrony Danych 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. Inspektor Ochrony Danych nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"** oraz oświadczenie o poufności- **załącznik nr 4 do Polityki Bezpieczeństwa.** Inspektor Ochrony Danych 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, Inspektor Ochrony Danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

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

§ 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 10 maja 2018 r ; Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z prztewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych) oraz ROZPORZĄDZENIE 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

§ 13.

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, zabraniem 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 Politykę Bezpieczeństwa i zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych:

a) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. , poz. 1000)

b) Rozporządzeniem Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z prztewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych)

c) 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);

d) Innymi przepisami mającymi zastosowania przy przetwarzaniu danych osobowych.

Podpis Administratora Danych Osobowych

WÓJT

.....

mgr Jacek Oględzki

Podpis

Podpis Inspektora Ochrony Danych

Klein Monika

.....

Podpis