ZARZĄDZENIE NR 99/2016
BURMISTRZA ZIĘBIC

z dnia 17 czerwca 2016 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Ziębicach

Na podstawie art. 36 oraz art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. 2015 r., poz. 2135, z późn. zm.) i art.33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. 2016 r., poz. 446) zarządza się, co następuje:

§ 1.

1. W Urzędzie Miejskim w Ziębicach wprowadza się dla zapewnienia ochrony przetwarzania danych osobowych:

1) Politykę bezpieczeństwa w Urzędzie Miejskim w Ziębicach - stanowiącą załącznik nr 1 do niniejszego zarządzenia,

2) Instrukcję zarządzania systemem informatycznym w Urzędzie Miejskim w Ziębicach -stanowiącą załącznik nr 2 do niniejszego zarządzania.

2. Dokumentacja, o której mowa w ust.1, ma zastosowanie do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym.

§ 2.

1. Z treścią dokumentów, o których mowa w § 1 ust.1 zobowiązani są zapoznać się wszyscy pracownicy Urzędu Miejskiego w Ziębicach przetwarzający dane osobowe.

2. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Ziębicach do przestrzegania zasad wynikających z dokumentów, o których mowa w paragrafie 1 ust.1.

§ 3.

Traci moc Zarządzenie Nr 42/2010 Burmistrza Ziębic z dnia 25.03.2010 roku w sprawie przyjęcia "Polityki Bezpieczeństwa" Urzędu Miejskiego w Ziębicach.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ ZIĘBIC
Alicja Bira

Załącznik nr 1 do zarządzenia nr 99/2016

Burmistrza Ziębic z dnia 17 czerwca 2016 roku

POLITYKA BEZPIECZEŃSTWA

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)

wdraża dokument o nazwie „Polityka Bezpieczeństwa".

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: Urząd Miejski w Ziębicach, 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, dostępnym 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, o których mowa w art. 3 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014r., poz. 1182, 1662, z 2015 r. poz. 1309), 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 danych osobowych,
8. **PODMIOCIE** – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową.

§ 3

1. Administrator Danych może wyznaczyć **(Administratora Bezpieczeństwa Informacji** celem nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

2. Upoważnienie dla **Administratora Bezpieczeństwa Informacji**, oraz zakres obowiązków 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

W podmiocie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują 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 Danych** stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. **Administrator Danych** nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**. Prowadzona jest dokumentacja opisująca 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 Danych** jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10

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

§ 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.**

§ 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 oddziałów, 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 niezbędne dokumenty wynikające z zapisów ustawy, oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

BURMISTRZ ZIĘBIC
Alicja Bira