ZARZĄDZENIE NR 2/17

Dyrektora Gminnego Ośrodka Kultury w Kwidzynie
z dnia 10 lutego 2017roku

w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Kwidzynie

Na podstawie 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 ze zmianami).

zarządzam, co następuję:

§ 1. Wprowadzam do stosowania Politykę bezpieczeństwa w Gminnym Ośrodku Kultury w Kwidzynie stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania i ma zastosowanie w przetwarzaniu danych osobowych w zbiorach manualnych oraz w systemach informatycznych.

Załącznik nr 1
Do Zarządzenia Nr 2/17
Dyrektora GOK z dnia 10 lutego 2017r.

POLITYKA BEZPIECZEŃSTWA
W GMINNYM OŚRODKU KULTURY W KWIDZYNIE

§ 1. 1. Polityka bezpieczeństwa w zakresie ochrony danych zwana dalej „ Polityką” , 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.

2. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

3. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zawiera:

a. identyfikację zasobów systemu tradycyjnego i informatycznego;
b. wykaz pomieszczeń, tworzący obszar, w którym przetwarzane są dane osobowe;
c. wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych;
d. opis struktury zbiorów danych i sposoby ich przepływu;
e. środki techniczne i organizacyjne, służące zapewnieniu poufności przetwarzanych danych.

§ 2. Ilekroć w „ Polityce Bezpieczeństwa” jest mowa o:

- Zbiorze danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów,
- Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
- Polityka- rozumie się przez to „ Polityka Bezpieczeństwa”,
- 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,

- Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

- Administratorze danych osobowych (ADO) – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Gminnym Ośrodku Kultury w Kwidzynie funkcję administratora danych pełni Dyrektor Ośrodka.

- Administratorze bezpieczeństwa informacji (ABI) – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony.

- Administrator systemu informatycznego (ASI)- rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzoru i przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego.

- Użytkownik– rozumie się przez to pracownika upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków,

§ 3. 1. Procedury i zasady określone w niniejszym dokumencie stosuje się do osób upoważnionych, do przetwarzania danych osobowych zatrudnionych w Gminnym Ośrodku Kultury w Kwidzynie.

2. Dyrektor jako Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji w celu nadzorowania i przestrzegania zasad ochrony danych osobowych chyba, że sam wykonuję te czynności. Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków określa załącznik do„ Polityki Bezpieczeństwa w Gminnym Ośrodku Kultury w Kwidzynie ” nr 1.

3. Wymagany jest wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa załącznik do „Polityki Bezpieczeństwa w Gminnym Ośrodku Kultury w Kwidzynie” nr 2.

4. Wymagany jest wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa załącznik do „Polityki Bezpieczeństwa w Gminnym ośrodku Kultury w Kwidzynie” nr 3.

5. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

i powiązania między nimi oraz sposoby przepływu danych pomiędzy poszczególnymi systemami określa załącznik do „Polityki Bezpieczeństwa w Gminnym ośrodku Kultury w Kwidzynie” nr 4.

6. Osoby, które przetwarzają dane w Gminnym Ośrodku Kultury w Kwidzynie, muszą posiadać upoważnionej do przetwarzania danych nadane przez Administratora Danych Osobowych oraz podpisać oświadczenie o zachowaniu poufności tych danych, określa załącznik do „Polityki Bezpieczeństwa w Gminnym Ośrodku Kultury w Kwidzynie” nr 5.

7. Ewidencja osób, przetwarzających dane osobowe w podmiocie posiadającym upoważnienie określa załącznik do „Polityki Bezpieczeństwa w Gminnym Ośrodku Kultury w Kwidzynie” nr 6 .

8. Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, określa załącznik do„Polityki Bezpieczeństwa w Gminnym Ośrodku Kultury
w Kwidzynie” nr 7.

9. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych.

10. Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz. W przypadku konieczności zniszczenia dokumentów zwierających dane osobowe, ich zniszczenie dokonuję się poprzez pocięcie w niszczarce.

11. Zasady przetwarzania danych osobowych w systemie informatycznym określona są w „ Instrukcji zarządzania systemami informatycznymi do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Kwidzynie”.

12. W przypadku otrzymania wniosku o udostępnianie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba przygotowuję odpowiedź w ciągu 30 dni.

13. W przypadku zbierania danych osobowych od osoby, której one dotyczą Administrator Danych

Osobowych

(lub osoba przez niego wyznaczona) jest obowiązany poinformować tę osobę o:

- Adresie swojej siedziby i pełnej nazwie,
- Celu zbierania danych,
- Prawie dostępu do treści swoich danych oraz ich poprawiania
- Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

§ 4. 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 Gminnym Ośrodku Kultury w Kwidzynie, 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. 1. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w Gminnym Ośrodku Kultury w Kwidzynie 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.

2. 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.

3. 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
   c. w sposób nieautoryzowany;
   d. rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   e. ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

4. Dla skutecznej realizacji Polityki Administrator Danych Osobowych 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.
   g. Monitorowanie zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

   h. ADO lub osoba przez niego upoważniona(ABI) wdraża wszystkie dokumenty składające się na Politykę Bezpieczeństwa i zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych.

§ 6. 1. ADO 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 ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ASI.

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:

a. środki ochrony fizycznej (np. drzwi ochronne, alarmy, monitoring);
b. środki techniczne (np. antywirus, podtrzymanie zasilania UPS) ;
c. środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym)

§7. 1. Nie przestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49-54a Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn.: Dz. U. z 2016 r. poz. 922 ze zm.).

2. W sprawach nieuregulowanych w niniejszej polityce, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych 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.

§8. Niniejszy dokument wchodzi w życie z dniem

…….. ……

Podpis Administratora Bezpieczeństwa Informacji Podpis Administratora Danych Osobowych

Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

…….
miejscowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

Na podstawie § 3 . Zarządzenia Nr 2/17 z dnia 10 lutego 2017 r.

Administrator Danych *(imię i nazwisko)*.....
powołuje w Gminnym Ośrodku Kultury w Kwidzynie
Administratora Bezpieczeństwa Informacji *(imię i nazwisko*)….....
…….PESEL.....

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

Zakres Obowiązków
Administratora Bezpieczeństwa Informacji

- 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.
- Zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.
- Prowadzić wszelką dokumentację opisującą sposób przetwarzania danych.
- Prowadzić ewidencję osób przetwarzających dane w posiadającym upoważnienie,
- Zestawiać dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Oświadczam, że zapoznałem/am się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako Administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w Gminnym Ośrodku Kultury w Kwidzynie zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz Ustawy o ochronie danych osobowych.

Administrator Danych — Administrator Bezpieczeństwa Informacji

…..... …….
Podpis *Podpis*

Załącznik nr 2 do Polityki Bezpieczeństwa
Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

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

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

Data i podpis Administratora Bezpieczeństwa Informacji

.....

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 3 do Polityki Bezpieczeństwa
Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

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

.....

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 4 do Polityki Bezpieczeństwa
Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

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

.....

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 5 do Polityki Bezpieczeństwa
Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z 29 sierpnia 1997r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2016r. poz. 922 ze zm.)

Upoważniam Panią/Pana

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 .....

Osoba upoważniona do przetwarzania danych, objętych zakresem , o których mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Administrator Danych	**Upoważniony**
….....	……..
Podpis	*Podpis*

Oświadczenie

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Gminnego Ośrodka Kultury w Kwidzynie .

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w Gminnym Ośrodku Kultury w Kwidzynie dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922) , w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

Administrator Danych	**Upoważniony**
….....	……..
Podpis	Data i podpis

Załącznik nr 6 do Polityki Bezpieczeństwa
Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

Ewidencja osób, przetwarzających dane osobowe w podmiocie posiadającym 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

.....

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 7 do
Polityki Bezpieczeństwa
Zarządzenia nr 2/17
Dyrektora GOK w Kwidzynie
z dnia 10 lutego 2017r.

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

.....

Data i podpis Administratora Danych Osobowych

.....