Gminny Ośrodek Kultury
w Krynkach
16-120 Krynki, ul. Grodzieńska 7
NIP 545-169-44-67
tel./fax 085 / 722 81 21

Zarządzenie nr. 3/2017
z dnia 15.03.2017
w sprawie wprowadzenia Polityki Bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Krynkach

**Na podstawie ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (tekst jedn. Dz. U. z 16 kwietnia 2012 r. poz. 406), ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 101 z 2002 r., poz. 926 z późn. zm.), § 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. z 2004 r. Nr 100, poz. 1024 ze zm.) zarządzam, co następuje:**

**&1**

**Z dniem 15.03.2017 r wprowadza się do stosowania „Politykę Bezpieczeństwa" i „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Krynkach, stanowiących odpowiednio załącznik nr. 1 , nr.2 do niniejszego Zarządzenia.**

**& 2**

**Polityka bezpieczeństwa określa zbiór zasad obowiązujących przy zbieraniu, przetwarzaniu danych osobowych we wszystkich zbiorach administrowanych przez Gminny Ośrodek Kultury w Krynkach**

**& 3**

**Zarządzenie wchodzi w życie z dniem 15.03.2017**

**Załączniki:**

**Zał. 1 Polityka bezpieczeństwa informacji Gminnego Ośrodka Kultury w Krynkach**

**Zał. 2 Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Ośrodku Kultury w Krynkach**

Dyrektor
Gminnego Ośrodka Kultury
*Elżbieta Stanisława Czeremcha*

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

Administrator Danych -Elżbieta Czeremcha

Dnia 15.03.2017 w podmiocie o nazwie GMINNY Ośrodek Kultury w Krynkach

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**
**wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją". Zapisy tego dokumentu wchodzą w życie z dniem 15.03.2017**

Ilekroć 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.

§ 1

Za przestrzeganie w Gminnym Ośrodku Kultury w Krynkach zapisów „instrukcji" odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji**

§2

W związku z tym, że w Gminnym Ośrodku kultury w Krynkach 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:

I

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.

II

1. 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.

2. 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.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

- poprzez zainstalowanie programu antywirusowego o nazwie .....
- poprzez zainstalowanie firewall (zapora sieciowa).
- poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. 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.

3. 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

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym (nr pokoju, nazwa działu)
.....
zaopatrzonym w system alarmowy (nazwa systemu, nazwa grupy interwencyjnej)
.....

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

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.

VI

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**

Podpis Administratora Danych Osobowych

Dyrektor
Gminnego Ośrodka Kultury
.....
Elżbieta Stanisława Czeremcha

Podpis

Podpis Administratora Bezpieczeństwa Informacji

# POLITYKA BEZPIECZEŃSTWA

Administrator Danych- Elżbieta Czeremcha

Dnia 15.03.2017 w podmiocie o nazwie Gminny Ośrodek Kultury w Krynkach

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". Zapisy tego dokumentu wchodzą w życie

z dniem15.03.2017

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Gminnym Ośrodku Kultury w Krynkach 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.
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 Gminnym Ośrodku Kultury w Krynkach 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** 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.

**Administratora 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** lub **Administratora Bezpieczeństwa Informacji**. **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"

§ 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**

Podpis Administratora Danych Osobowych

Dyrektor
Gminnego Ośrodka Kultury
Elżbieta Stanisława Czeremcha

.....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

.....

Podpis

.....

*miejscowość i data*

**Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków**

załącznik nr 1 do „Polityki Bezpieczeństwa"

**Na podstawie** § 2. Polityki Bezpieczeństwa z dnia ..... 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**

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)

**Administrator Danych** *(imię i nazwisko)*.....powołuje w

podmiocie *(nazwa firmy)*.....NIP:.....

**Administratora Bezpieczeństwa Informacji** *(imię i nazwisko)*.....

pesel.....

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, zabraniem 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** nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**.

**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 § 3. „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 § 4. „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 § 5. „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 § 7. „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 podmiocie..... zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

**Administrator Bezpieczeństwa Informacji**

.....

*Podpis*

**Administrator Danych**

.....

# „Procedura Alarmowa"

Administrator Danych – Elżbieta Czeremcha
Dnia 15.03.2917 w podmiocie o nazwie Gminny Ośrodek Kultury w Krynkach

w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych

na podstawie art. 36.1. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)
wdraża dokument o nazwie **„Procedura Alarmowa"**.

Zapisy tego dokumentu wchodzą w życie
z dniem 15.03.2017

Definicje:
**Uchybienie** - *świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.*
**Zagrożenie** - *świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.*
**ABI** - *Administrator Bezpieczeństwa Informacji*
**ADO** - *Administrator Danych Osobowych*

## 1. Procedura alarmowa

Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje **„Dziennik Uchybień i Zagrożeń"**, związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem. Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości. Integralną częścią Procedury Alarmowej jest „**Dziennik Uchybień i Zagrożeń"** - (załącznik nr 1), **„Protokół Zagrożenia"** - (załącznik nr 2), **„Protokół Uchybienia"** - (załącznik nr 3), prowadzony przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

## 2. Charakterystyka możliwych „Uchybień i Zagrożeń"

I. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne
Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników podmiotu lub osób nie będących pracownikami podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:
- *niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,*
- *niewłaściwe zabezpieczenie sprzętu komputerowego,*
- *dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,*
- *pomyłki informatyków,*
- *kradzież danych,*
- *kradzież sprzętu informatycznego,*
- *działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do*
*utraty danych osobowych lub uszkodzenia nośników danych.*

II. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne
Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników
podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub

naruszenia ich poufności. W szczególności są to działania takie jak:
- *celowe zniszczenie danych osobowych lub nośników danych,*
- *kradzież danych osobowych,*
- *dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,*
- *kradzież danych,*
- *kradzież sprzętu informatycznego,*
- *działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do*
*utraty danych osobowych lub uszkodzenia nośników danych.*

III. Uchybienia i zagrożenia losowe

Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do
zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to sytuacje takie jak:
- *klęski żywiołowe,*
- *przerwy w zasilaniu,*
- *awarie serwera,*
- *pożar,*
- *zalanie wodą.*

## 3. Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

Każdy pracownik podmiotu posiadający upoważnienie do przetwarzania danych osobowych, w przypadku
stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Danych.

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **uchybienia** ma obowiązek:
1. odnotować każde uchybienie w „**Dzienniku Uchybień i Zagrożeń"**
2. sporządzić **„Protokół Uchybienia"**
3. wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **zagrożenia** ma obowiązek:
1. zabezpieczyć dowody, powiadomić policję (w przypadku włamania)
2. zabezpieczyć dane osobowe oraz nośniki danych
3. odnotować każde zagrożenie w „**Dzienniku Uchybień i Zagrożeń"**
4. sporządzić **„Protokół Zagrożenia"**
5. wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia
6. powiadomić o zaistniałej sytuacji Administratora Danych
7. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia
8. ADO wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie

Dyrektor
Gminnego Ośrodka Kultury
Elżbieta Stanisława Czeremcha

## „Dziennik Uchybień i Zagrożeń"

*(załącznik nr 1 do Procedury Alarmowej)*

| Kod | Data i godzina zdarzenia | Rodzaj zdarzenia *(uchybienie/ zagrożenie)* | Opis zdarzenia | Skutki zdarzenia | Działania naprawcze | Podpis ABI |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Nazwa i adres podmiotu

.....

Miejscowość i data

# „Protokół Zagrożenia"

*(załącznik nr 2 do Procedury Alarmowej)*

**Data i godzina wystąpienia zagrożenia**

.....

**Kod zagrożenia**

.....

**Opis zagrożenia**

.....
.....
.....
.....
.....

**Przyczyny powstania zagrożenia**

.....
.....
.....
.....
.....

**Zaistniałe skutki zagrożenia**

.....
.....
.....
.....
.....

**Podjęte działania naprawczo-zapobiegawcze**

.....
.....
.....
.....
.....

**Administrator Bezpieczeństwa Informacji**

.....

Podpis

**Administrator Danych Osobowych**

.....

Podpis

Nazwa i adres podmiotu

.....

Miejscowość i data

# „Protokół Uchybienia"

*(załącznik nr 3 do Procedury Alarmowej)*

**Data i godzina wystąpienia uchybienia**.....

**Kod uchybienia**

.....

**Opis uchybienia**

.....
.....
.....
.....
.....

**Przyczyny powstania uchybienia**

.....
.....
.....
.....
.....

**Zaistniałe skutki uchybienia**

.....
.....
.....
.....
.....

**Podjęte działania naprawczo-zapobiegawcze**

.....
.....
.....
.....
.....

**Administrator Bezpieczeństwa Informacji**

.....
Podpis

**Administrator Danych Osobowych**

.....
Podpis

# „Raport roczny"

*(załącznik nr 1 do „Sprawozdania rocznego stanu systemu ochrony danych osobowych")*

| Nazwa i adres podmiotu<br><br>..... | Miejscowość i data<br><br>..... |
|---|---|

| **Zagadnienia omawiane na zebraniu** | **Uwagi/wnioski** |
|---|---|
| Podsumowanie realizacji wytycznych z poprzedniego „Sprawozdania rocznego stanu systemu ochrony danych osobowych" | |
| Omówienie zmian procedur w systemie oraz zmian w systemie informatycznym | |
| Omówienie Dziennika Uchybień i Zagrożeń | |
| Wnioski oraz zadania do realizacji | |

| | |
|---|---|
| | |

| Uczestnicy zebrania | Podpis uczestnika |
|---|---|
| | |

| Podpis ABI | Podpis ADO |
|---|---|
| | |