BIBLIOTEKA I OŚRODEK KULTURY
w Piotrkowie Kujawskim
ul. Rynek 20, 88-230 Piotrków Kuj.
tel. 54 265-41-85
NIP 889-151-45-83 REGON 364319136

ZARZĄDZENIE Nr 30/2016

DYREKTORA BIBLIOTEKI I OŚRODKA KULTURY W PIOTRKOWIE KUJAWSKIM

z dnia 06 maja 2016 roku

w sprawie wprowadzenia "Procedury alarmowej"
w Bibliotece i Ośrodku Kultury w Piotrkowie Kujawskim.

§1

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) zarzadzam wprowadzenie dokumentu o nazwie **„Procedura Alarmowa"** w Bibliotece i Ośrodku Kultury w Piotrkowie Kujawskim, który stanowi załącznik nr 1 do niniejszego zarządzenia.

§2

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od dnia 1 maja 2016 roku.

DYREKTOR
mgr Joanna Lewandowska-Kołodziejska

Załącznik nr 1
do Zarządzenia nr 30/2016
z dnia 06 maja 2016r.

„Procedura Alarmowa"

Administrator Danych Joanna Lewandowska - Kołodziejska
Dnia 06 maja 2016r. w podmiocie o nazwie Biblioteka i Ośrodka Kultury w Piotrkowie Kujawskim 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 01 maja 2016r.

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 Danych.

Administrator Danych 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 Danych 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. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia
7. ADO wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie

4. **Rejestr Uchybień i Zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie:**
5.

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ADO, który sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ADO. ADO sporządza protokół uchybienia.

3	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ADO, który sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ADO, który powinien sprawdzić system uwierzytelniania oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ADO sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ADO, który powinien zabezpieczyć nośnik danych i sporządza protokół zagrożenia.
6	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ADO, który powinien zabezpieczyć dane i sporządza protokół zagrożenia.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ADO, który sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić ADO, ktory powinien zabezpieczyć pomieszczenie i sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić ADO, ktory sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ADO sporządza protokół zagrożenia.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. ADO powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
11	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ADO, który powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ADO sporządza protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ADO, który sprawdza stan uszkodzeń, zabezpiecza dowody i sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ADO, który sprawdza stan uszkodzeń, zabezpiecza dowody i sporządza protokół zagrożenia.

14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ADO, który powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej i sporządza protokół zagrożenia.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ADO, który sporządza protokół uchybienia.
16	Zdarzenia losowe	Należy oszacować powstale straty i sporządzić protokół zagrożenia lub uchybienia.

DYREKTOR

mgr Joanna Lewandowska-Kołodziejska

„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 Danych Osobowych

.....

Podpis

BIBLIOTEKA I OŚRODEK KULTURY
w Piotrkowie Kujawskim
ul. Rynek 20, 88-230 Piotrków Kuj.
tel. 54 265-41-85
NIP 889-151-45-83 REGON 364319136

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 Danych Osobowych

.....

Podpis