Gminna Biblioteka Publiczna w Zakrzówku
ul. Żeromskiego 24 B, 23–213 Zakrzówek
tel/fax: (81) 821–50–36
biblioteka@zakrzowek.gmina.pl
www.gbp.zakrzowek.gmina.pl

GMINNA BIBLIOTEKA
PUBLICZNA W ZAKRZÓWKU

PROCEDURA ALARMOWA

GMINNEJ BIBLIOTEKI PUBLICZNEJ W ZAKRZÓWKU ORAZ FILII W STUDZIANKACH, SULOWIE I RUDNIKU DRUGIM

Wydanie: 02

PROCEDURA ALARMOWA

Administrator Danych: **Teresa Stankiewicz, Dyrektor Gminnej Biblioteki Publicznej w Zakrzówku** dnia 01 lutego 2015 r. w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36.1. ustawy z dania 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz Dz. U. 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 wdrożenia.

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

I. 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 również ograniczenie ich powstania w przyszłości. Integralną częścią Procedury Alarmowej są:

- „**Dziennik Uchybień i Zagrożeń**" – załącznik nr 1;
- „**Protokół Zagrożenia**" – załącznik nr 2;
- „**Protokół Uchybienia**" – załącznik nr 3;

prowadzone przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

II. Charakterystyka możliwych „Uchybień i Zagrożeń"

1. 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,*
- *działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.*

2. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne

Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe 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:

- *celowe zniszczenie nośników danych osobowych*
- *dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,*
- *kradzież danych osobowych,*
- *kradzież sprzętu informatycznego,*
- *działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.*

3. 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 działania takie jak:

- *klęski żywiołowe,*
- *przerwy w zasilaniu,*
- *awarie serwera,*
- *pożar,*
- *zalanie wodą.*

III. 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 Osobowych
7. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia
8. Administrator Danych Osobowych konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie

IV. Rejestr Uchybień i Zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie

Kod uchybienia lub zagrożenia	Uchybienie i zagrożenie 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 ABI, który sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI, który sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI, który sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ABI, który powinien sprawdzić system uwierzytelniania oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć nośnik danych i powiadomić ADO, ABI sporządza protokół zagrożenia.
6	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i powiadomić ADO, ABI sporządza protokół zagrożenia.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI, który sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół zagrożenia.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. ABI 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 ABI. ABI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ABI sporządza protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ABI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI powiadamia ADO i sporządza protokół zagrożenia.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe straty i sporządzić protokół zagrożenia lub uchybienia.

Gminna Biblioteka Publiczna w Zakrzówku	**Załącznik nr 1 do Procedury Alarmowej**	**Wydanie: 02**
	Obowiązuje od: 01 lutego 2015 r.	**Strona 1 z 1**

Dziennik Uchybień i Zagrożeń

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia (uchybienie lub zagrożenie)	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis ABI

Niniejszy dokument zatwierdzono do stosowania
w Gminnej Bibliotece Publicznej w Zakrzówku.

Protokół Zagrożenia

Data i godzina wystąpienia zagrożenia: ……

Kod zagrożenia: ……

Opis zagrożenia:

……..
……..
……..
……..
……..
……..

Przyczyny powstania zagrożenia:

……..
……..
……..
……..
……..
……..

Zaistniałe skutki zagrożenia:

……..
……..
……..
……..
……..
……..

Podjęte działania naprawczo-zapobiegawcze:

……..
……..
……..
……..
……..
……..

Administrator Bezpieczeństwa Informacji **Administrator Danych Osobowych**

…….. ……

Niniejszy dokument zatwierdzono do stosowania
w Gminnej Bibliotece Publicznej w Zakrzówku.

Protokół Uchybienia

Data i godzina wystąpienia uchybienia: ……

Kod uchybienia: ……

Opis uchybienia:

……..
……..
……..
……..
……..
……..

Przyczyny powstania uchybienia:

……..
……..
……..
……..
……..
……..

Zaistniałe skutki uchybienia:

……..
……..
……..
……..
……..
……..

Podjęte działania naprawczo-zapobiegawcze:

……..
……..
……..
……..
……..
……..

Administrator Bezpieczeństwa Informacji ……..

Administrator Danych Osobowych ……

Niniejszy dokument zatwierdzono do stosowania
w Gminnej Bibliotece Publicznej w Zakrzówku.