Zarządzenie Nr 7/2017
Dyrektora Centrum Usług Wspólnych w Okonku
z dnia 4 stycznia 2017

w sprawie wprowadzenia Procedury alarmowej i ustalenia zasad sporządzania sprawozdania rocznego stanu systemu ochrony danych osobowych w Centrum Usług Wspólnych w Okonku.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z póź. zm.) zarządza się, co następuje:

§ 1. Wprowadza się do użytku „Procedurę alarmową" dotyczącą ochrony danych osobowych, stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Ustala się zasady sporządzania „Sprawozdania rocznego stanu systemu ochrony danych osobowych", stanowiącego załącznik nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje się pracowników Centrum Usług Wspólnych w Okonku do zapoznania się oraz do stosowania zasad określonych w § 1 i § 2.

§ 4. Nadzór nad wykonaniem zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji w Centrum Usług Wspólnych w Okonku.

DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

Załącznik nr 1

„Procedura Alarmowa"

DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

Administrator Danych.

Dnia 02.01.2017 w podmiocie o nazwie .
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 02.01.2017

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

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

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 ABI. ABI sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI 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. ABI 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, 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 starty i sporządzić protokół zagrożenia lub uchybienia.

„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 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 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

Załącznik nr 6

„Sprawozdanie roczne stanu systemu ochrony danych osobowych"

Administrator Danych.....

Dnia ..... w podmiocie o nazwie .....

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

„Sprawozdanie roczne stanu systemu ochrony danych osobowych".

Zapisy tego dokumentu wchodzą w życie

z dniem .....

1. *„Sprawozdanie roczne stanu systemu ochrony danych osobowych" przeprowadza się raz w roku,* z datą rok od chwili wejścia w życie tego dokumentu. *Osobą odpowiedzialną za przygotowanie sprawozdania rocznego w podmiocie jest ABI. Sprawozdanie roczne przygotowuje się na podstawie dokumentu o nazwie* ***„Raport roczny"****, który stanowi załącznik nr 1 do „Sprawozdania rocznego stanu systemu ochrony danych osobowych" w podmiocie. Po przeprowadzeniu analizy stanu ochrony danych osobowych w podmiocie oraz uzupełnieniu „Raportu rocznego" ABI zwołuje zebranie, w którym uczestniczą: ABI, ADO i kierownicy działów lub referatów, w których przetwarzane są dane osobowe. Podczas zebrania ABI przedstawia uczestnikom stan zabezpieczeń, stan infrastruktury informatycznej, „Dziennik uchybień i zagrożeń" oraz omawiane są procedury zabezpieczające podmiot przed sytuacjami, w których może dojść do zniszczenia danych, wycieku danych lub naruszenia ich poufności.*

„Raport roczny"

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

Nazwa i adres podmiotu	Miejscowość i data .....

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