BURMISTRZ
Miasta Sandomierza

ZARZĄDZENIE NR 121/2015/ABI
Burmistrza Miasta Sandomierza
z dnia 7 grudnia 2015r.

w sprawie wprowadzenia Procedury alarmowej i ustalenia zasad sporządzania Sprawozdania rocznego stanu systemu ochrony danych osobowych w Urzędzie Miejskim w Sandomierzu.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze 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 Urzędu Miejskiego w Sandomierzu do zapoznania się oraz do stosowania zasad określonych w § 1 i § 2.

§4

Nadzór nad wykonaniem zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji w Urzędzie Miejskim w Sandomierzu.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Sandomierza
mgr Marek Bronkowski

Administrator Bezpieczeństwa Informacji
mgr Marzena Wieczorek

Załącznik nr 1
do Zarządzenia Nr
121/2015/ABI
Burmistrza Miasta Sandomierza

Administrator Danych Osobowych w Urzędzie Miejskim w Sandomierzu w celu pełnej kontroli oraz zapobiegania możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze zm.) wprowadza dokument o nazwie **„Procedura Alarmowa"**. Zapisy tego dokumentu obowiązują wszystkich pracowników Urzędu Miejskiego w Sandomierzu , którzy przetwarzają dane osobowe w systemach informatycznych i w wersji papierowej.

Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

1. Podstawowe definicje i pojęcia

UM – Urząd Miejski w Sandomierzu

ADO - Administrator Danych Osobowych – Burmistrz Miasta Sandomierza.

ABI - Administrator Bezpieczeństwa Informacji osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Bezpieczeństwa Informacji.

ASI- Administrator Systemu Informatycznego.

Użytkownik danych – każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie.

Osoba upoważniona – osoba posiadająca upoważnienie wydane przez ABI lub osobę uprawnioną przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu.

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.

Procedura alarmowa – sposób postępowania (rodzaj czynności) osób funkcyjnych i pracowników w sytuacji zagrożenia utraty danych osobowych przetwarzanych w Urzędzie Miejskim w Sandomierzu.

2.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 UM w Sandomierzu.

3.Charakterystyka możliwych „Uchybień i Zagrożeń"

I. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne. Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania użytkowników danych lub osób nie będących pracownikami Urzędu Miejskiego w Sandomierzu, 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 użytkowników danych, 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.

4. 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 ABI lub ADO.

ABI 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.

ABI 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 ADO,
7) podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia,
8) ADO wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie.

5. **Rejestr Uchybień i Zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w Urzędzie Miejskim w Sandomierzu.**

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.
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. ABI i ASI 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. ASI 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

13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI i ASI. ASI 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 ASI i ABI. ABI sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe starty i sporządzić protokół zagrożenia lub uchybienia.

Burmistrz Sandomierza

mgr Marek Bronkowski

„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

Sandomierz, data

Urząd Miejski w Sandomierzu

„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 **Administrator Danych Osobowych**

....

Podpis Podpis

Sandomierz, data

Urząd Miejski w Sandomierzu

„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 2
do Zarządzenia
nr 121/2015/ABI
Burmistrza Miasta
Sandomierza
z dnia 7.12.2015r.

Sprawozdanie roczne stanu systemu ochrony danych osobowych

W celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanych z ochroną danych osobowych na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych Administrator Danych wdraża dokument o nazwie "Sprawozdanie roczne stanu systemu ochrony danych osobowych".

1. Sprawozdanie roczne stanu systemu ochrony danych osobowych przeprowadzać się będzie od 2015 r. raz w roku. Osobą odpowiedzialną za przygotowanie sprawozdania jest ABI. Sprawozdanie roczne przygotowuje się na podstawie dokumentu „Raport roczny", który stanowi załącznik nr 1.
2. Po przeprowadzeniu analizy stanu ochrony danych osobowych ABI uzupełnia raport roczny i zwołuje zebranie w którym uczestniczą: ADO, ABI, pracownicy Urzędu Miejskiego w Sandomierzu, którzy wykonując czynności służbowe, przetwarzają dane osobowe, tzn. wykonują na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie.
3. Podczas zebrania ABI przedstawia uczestnikom stan zabezpieczeń, stan infrastruktury informatycznej, „Dziennik uchybień i zagrożeń" oraz omawiane są procedury zabezpieczające Urząd Miejski w Sandomierzu przed sytuacjami, w których może dojść do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

Załącznik nr 1
do „Sprawozdania rocznego stanu
systemu ochrony danych osobowych"

„Raport roczny"

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