Zarządzenie Nr 101/2015

Burmistrza Trzebiatowa

z dnia 28 października 2015 r.

w sprawie wprowadzenia Procedury alarmowej i ustalenia zasad sporządzania sprawozdania rocznego stanu systemu ochrony danych osobowych w ramach „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Trzebiatowie"

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2015 r., poz. 1515) w związku z art. 36 ust. 12 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) zarządzam, co następuje:

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

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

§ 3. Zobowiązuje się pracowników Urzędu Miejskiego w Trzebiatowie do stosowania zasad określonych w w/w dokumentach.

§ 4. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
TRZEBIATOWA
Zdzisław Matasewicz

Załącznik nr 1
do Zarządzenia nr 101/2015
Burmistrza Trzebiatowa
z dnia 28 października 2015 r.

Procedura alarmowa

1. Wstęp

Administrator Danych Osobowych w Urzędzie Miejskim w Trzebiatowie w celu pełnej kontroli oraz zapobiegania możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) wprowadza dokument o nazwie **„Procedura Alarmowa"**.

Zapisy tego dokumentu obowiązują wszystkich pracowników Urzędu Miejskiego w Trzebiatowie, którzy przetwarzają dane osobowe w systemach informatycznych i w wersji papierowej.

Z niniejszym dokumentem powinni zapoznać się wszyscy pracownicy.

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

Dokument powinien zostać umieszczony w formie elektronicznej, na wewnętrznych zasobach sieciowych Urzędu Miejskiego, do których dostęp posiadają wszyscy pracownicy Urzędu Miejskiego w Trzebiatowie lub w uzasadnionych przypadkach na żądanie powinien zostać im przedłożony w formie papierowej.

2. Podstawowe definicje i pojęcia

ABI - Administrator Bezpieczeństwa Informacji
ADO - Administrator Danych Osobowych
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 Trzebiatowie.

3. 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.

4. Charakterystyka możliwych „Uchybień i Zagrożeń"

4.1. 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,
- 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.

4.2. 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.

4.3. 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 sytuacje takie jak:
- klęski żywiołowe,
- przerwy w zasilaniu,
- awarie serwera,
- pożar,
- zalanie wodą.

5. 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:
a. odnotować każde uchybienie w **„Dzienniku Uchybień i Zagrożeń"**
b. sporządzić **„Protokół Uchybienia"**
c. wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **zagrożenia** ma obowiązek:
a. zabezpieczyć dowody, powiadomić policję (w przypadku włamania)
b. zabezpieczyć dane osobowe oraz nośniki danych
c. odnotować każde zagrożenie w **„Dzienniku Uchybień i Zagrożeń"**
d. sporządzić **„Protokół Zagrożenia"**
e. wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia
f. powiadomić o zaistniałej sytuacji Administratora Danych
g. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia
h. ADO wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie

6. 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 straty i sporządzić protokół zagrożenia lub uchybienia.

Załącznik nr 1
do Procedury Alarmowej

Dziennik Uchybień i Zagrożeń

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

Załącznik nr 2
do Procedury Alarmowej

Urząd Miejski w Trzebiatowie
ul. Rynek 1
72-320 Trzebiatów

Trzebiatów, ...

Protokół Zagrożenia

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

Załącznik nr 3
do Procedury Alarmowej

Urząd Miejski w Trzebiatowie
ul. Rynek 1
72-320 Trzebiatów

Trzebiatów, ...

Protokół Uchybienia

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 101/2015
Burmistrza Trzebiatowa
z dnia 28 października 2015 r.

Sprawozdanie roczne stanu systemu ochrony danych osobowych

Administrator Danych w Urzędzie Miejskim w Trzebiatowie w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) wdraża dokument o nazwie

„Sprawozdanie roczne stanu systemu ochrony danych osobowych"

„Sprawozdanie roczne stanu systemu ochrony danych osobowych" przeprowadza się raz w roku za rok poprzedni w terminie do 31 stycznia roku następnego.
Osobą odpowiedzialną za przygotowanie sprawozdania rocznego w podmiocie jest ABI. Sprawozdanie roczne przygotowuje się na podstawie dokumentu o nazwie **„Raport roczny",** który stanowi załącznik 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.

Załącznik
do „Sprawozdania rocznego
stanu systemu ochrony
danych osobowych"

Raport roczny

Urząd Miejski w Trzebiatowie Ul. Rynek 1 72-320 Trzebiatów	Trzebiatów,

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