PROCEDURA ALARMOWA

Uzupełnienie Polityki Bezpieczeństwa w podmiocie

Administrator Danych Osobowych – **Burmistrz Miasta i Gminy Frombork**

dnia 23 marca 2016 roku w podmiocie o nazwie: **Urząd Miasta i Gminy we Fromborku**
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 (t.j. Dz. U. 2014 r., poz. 1182, zm. poz. 1662 oraz z 2015 r. poz. 1309.)
wdraża dokument o nazwie Procedura Alarmowa.

§ 1. Ilekroć w Procedurze Alarmowej jest mowa o:

1. **UCHYBIENIU -** świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych,
2. **ZAGROŻENIU -** świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych,
3. **ADO -** Administrator Danych Osobowych.

§ 2. 1. Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje **Dziennik Uchybień i Zagrożeń**, związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem.

2. 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.
3. Integralną częścią Procedury Alarmowej jest:
   1) Dziennik Uchybień i Zagrożeń - **załącznik nr 1 do Procedury Alarmowej,**
   2) Protokół Zagrożenia - **załącznik nr 2 do Procedury Alarmowej**,
   3) Protokół Uchybienia - **załącznik nr 3 do Procedury Alarmowej**,

   prowadzony przez Informatyka w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

§ 3. Charakterystyka możliwych „Uchybień i Zagrożeń":

1. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne:
   1) 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:
   a) niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
   b) niewłaściwe zabezpieczenie sprzętu komputerowego,
   c) dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
   d) pomyłki informatyków,
   e) kradzież danych,
   f) kradzież sprzętu informatycznego,
   g) działanie wirusów i innego szkodliwego oprogramowania
   h) oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

2. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne:
   1) 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:
   a) celowe zniszczenie danych osobowych lub nośników danych,
   b) kradzież danych osobowych,
   c) dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
   d) kradzież danych,
   e) kradzież sprzętu informatycznego,
   f) działanie wirusów i innego szkodliwego oprogramowania
   g) oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

3. Uchybienia i zagrożenia losowe:
   1) 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:
   a) klęski żywiołowe,
   b) przerwy w zasilaniu,
   c) awarie serwera,
   d) pożar,
   e) zalanie wodą.

§ 4. Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

1. Każdy pracownik podmiotu posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Informatyka lub Administratora Danych Osobowych.
2. Informatyk 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.

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