Instrukcja postępowania na wypadek incydentu bezpieczeństwa danych osobowych

Cieszyński Ośrodek Kultury „Dom Narodowy"

Rynek 12

43-400 Cieszyn

Zatwierdzenie dokumentu: 11.05.2017 r.

sporządził: Janusz Dębowski

ABI/DPO/IOD/Audytor
Janusz Dębowski

zatwierdził: Administrator Danych

DYREKTOR
COK "DOM NARODOWY"
mgr Monika Sikora-Monkiewicz

Spis treści

1. Postanowienia ogólne.....3
2. Postępowanie w przypadku naruszenia lub podejrzeniu naruszenia zabezpieczenia systemu ochrony danych osobowych 4

1. Postanowienia ogólne.

1.1. Niniejsza „Instrukcja postępowania na wypadek incydentu bezpieczeństwa danych osobowych" określa tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych lub powzięcia podejrzenia o takim naruszeniu. Dokument ten jest elementem dokumentacji bezpieczeństwa danych osobowych. Użyte w nim terminy zostały zdefiniowane w Polityce bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.

1.2. Przestrzeganie postanowień niniejszej instrukcji ma służyć wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych.

1.3. Naruszenie ochrony danych osobowych, może być spowodowane:

a) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;

b) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;

c) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.

1.4. Za incydent bezpieczeństwa danych osobowych uważa się w szczególności:

a) brak możliwości fizycznego dostępu do danych np.: zagubiony klucz do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.;

b) brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć;

c) zmienioną zawartość zbioru, niepoprawną treść, postać, data, różnicę w danych itp.;

d) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;

e) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;

f) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych;

g) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;

h) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;

i) próba nielegalnego logowania się do systemu lub włamania do systemu;

j) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych,

k) niesprawne działanie lub nieuprawnione wyłączenie jakiegokolwiek elementu systemu zabezpieczeń,

l) wystąpienie warunków, które stwarzają zagrożenie dla przechowywanych danych (zbyt wysoka temperatura, nadmierna wilgotność, pole elektromagnetyczne lub elektrostatyczne),

m) stan pomieszczeń, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieuprawnione.

2. Postępowanie w przypadku naruszenia lub podejrzeniu naruszenia zabezpieczenia systemu ochrony danych osobowych .

2.1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na wystąpienie incydentu bezpieczeństwa informacji, które zostały opisane w "Postanowieniach ogólnych" niniejszej instrukcji, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz Administratora Danych.

2.2. Użytkownik do momentu przybycia Administratora Danych bądź upoważnionej przez niego osoby powinien:

a) zabezpieczyć dostęp do pomieszczenia lub urządzenia,
b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony,
c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony,
d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych lub osoby upoważnionej.

2.3. Po przybyciu na miejsce, o którym mowa w pkt. 2.1, Administrator Danych lub osoba przez niego upoważniona następujące czynności:

a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych,
b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia,
c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony,
d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń.

2.4. W przypadku zakwalifikowaniu zdarzenia jako "incydent bezpieczeństwa" użytkownik w porozumieniu z Administratorem Danych przygotowuje "Notatkę z incydentu bezpieczeństwa":

a) Notatka powinna zawierać wnioski określające zakres działań organizacyjnych i technicznych pozwalających zlikwidować skutki incydentu,
b) notatka powinna zawierać opis środków zapobiegających w przyszłości naruszeniom bezpieczeństwa danych osobowych,
c) Administrator Danych gromadzi notatki jako dowód na wystąpienie zdarzeń oraz sposobów postępowania,
d) wzór notatki określony jest w załączniku nr 1 do niniejszej instrukcji.