Załącznik nr 2 do Zarządzenia nr 19/2018
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie w Toruniu
z dnia 16 marca 2018 r. w sprawie wprowadzenia w MOPR w Toruniu
Polityki Bezpieczeństwa Danych Osobowych

Instrukcja
postępowania w sytuacji naruszenia ochrony danych osobowych w systemach komputerowych
w Miejskim Ośrodku Pomocy Rodzinie w Toruniu

§ 1

Niniejsza instrukcja przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych i określa zasady i tryb postępowania w sytuacji naruszenia ochrony danych osobowych, jeżeli:

1. stwierdzono naruszenie bezpieczeństwa systemu informatycznego;
2. istnieje podejrzenie naruszenia zabezpieczeń ochrony danych osobowych.

§ 2

Podejrzenie naruszenia ochrony danych osobowych

Podejrzenie naruszenia danych osobowych występuje każdorazowo gdy:

1. Zostaje stwierdzone naruszenie zabezpieczeń stałych, w tym miedzy innymi:
   a) włamanie lub próba włamania;
   b) naruszenie plomb w komputerach lub elementach sieci komputerowej;
   c) otwarcie przed rozpoczęciem pracy drzwi pomieszczeń, w których odbywa się przetwarzanie danych osobowych lub zainstalowane są urządzenia komputerowe i elementy sieci komputerowej;
   d) wybite lub otwarte przed rozpoczęciem pracy okno w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych lub zainstalowane są urządzenia komputerowe i elementy sieci komputerowej.
2. W czasie pracy systemu komputerowego, na którym odbywa się przetwarzanie danych osobowych występują nieprawidłowości, w tym przede wszystkim:
   a) stwierdzono obecność „wirusa" komputerowego;
   b) komputer lub elementy sieci komputerowej wykazują błędne działanie;
   c) pojawią się trudności z uruchomieniem komputera lub z wejściem do sieci komputerowej;
   d) stwierdzono naruszenie hasła dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm hasła);
   e) sposób działania programu odbiega od „normy";
   f) zawartość informacyjna całej bazy danych lub jej część jest niezgodna ze stanem faktycznym lub podlega niezamierzonym zmianom;
   g) powstają trudności z zapisem danych na nośnikach informacji lub trudności z ich odczytem;
   h) następuje zanik lub wyłączenia napięcia zasilającego.
3. W trakcie okresowych przeglądów i testów komputerów zostają wykryte nieprawidłowości, w tym miedzy innymi:
   a) uszkodzenia sprzętu komputerowego i elementów sieci komputerowej;
   b) błędne wejście i wyjście z sieci komputerowej;

c) nieuzasadnione włączenie i wyłączenie komputera zarządzającego siecią komputerową;
d) zainfekowanie „wirusami" komputerowymi nośników danych aktualnie użytkowanych lub przeznaczonych do przechowywania kopii archiwalnych;
e) naruszenie plomb w komputerach lub sieci komputerowej;
f) niespójność lub nieprawidłowość informacji zapisanej w bazie danych;
g) brak odpowiedniej, dokumentacji technicznej i użytkowej.

4. Administrator bezpieczeństwa informacji wejdzie w posiadanie informacji o naruszeniu obowiązujących procedur związanych z przetwarzaniem danych osobowych, w tym miedzy innymi z:
   a) przekazywaniem lub udostępnianiem danych osobowych podmiotom nieupoważnionym do ich posiadania;
   b) nieobecnością pracowników w otwartych pomieszczeniach, w których odbywa się przetwarzanie danych osobowych;
   c) brakiem okresowej archiwizacji danych;
   d) nie zniszczonymi zbędnymi lub uszkodzonymi wydrukami komputerowymi oraz nośnikami informacji;
   e) brakiem nadzoru lub nieprawidłowościami w postępowaniu z nośnikami zawierającymi dane osobowe podczas ich naprawy;
   f) przekazywaniem i udostępnianiem oprogramowania użytkowego lub jego modyfikowaniem albo rozszyfrowywaniem.

§ 3

Naruszenie ochrony danych osobowych

Naruszenie ochrony danych osobowych ma miejsce wtedy, gdy istnieje pewność, że ochrona danych osobowych została naruszona. Przypadki naruszenia ochrony danych osobowych przedstawione są w § 2.

§ 4

Procedura postępowania w sytuacji podejrzenia naruszenia ochrony danych osobowych

1. W przypadku podejrzenia naruszenia ochrony danych osobowych należy powiadomić Dyrektora Miejskiego Ośrodka Pomocy Rodzinie oraz administratora bezpieczeństwa informacji o zaistniałej sytuacji.

2. Jeżeli stwierdzono naruszenie zabezpieczeń stałych należ:
   a) ustalić przyczynę naruszenia zabezpieczeń;
   b) skontrolować sprawność techniczną sprzętu komputerowego i elementów sieci komputerowej;
   c) skontrolować procedury uruchamiania komputera, wejścia do sieci oraz uruchamiania oprogramowania użytkowego;
   d) przeprowadzić procedury testujące na obecność „wirusów" komputerowych;
   e) sprawdzić kompletność bazy danych.

3. Jeżeli stwierdzono nieprawidłowości w działaniu systemu informatycznego należy:
   a) ustalić przyczynę nieprawidłowości w działaniu systemu informatycznego;
   b) sprawdzić zabezpieczenia stałe;
   c) przeprowadzić procedury testujące na obecność „wirusów" komputerowych;

d) uruchomić procedury testujące sprzętu komputerowego, elementy sieci komputerowej oraz oprogramowania użytkowego;
e) sprawdzić kompletność bazy danych.

4.Jeżeli stwierdzono nieprawidłowości w użytkowaniu bazy danych zawierających dane osobowe lub naruszenie obowiązujących procedur związanych z przetwarzaniem danych osobowych należy:

a) sprawdzić, czy informacja podlegająca ochronie nie została udostępniona podmiotom nieupoważnionym do ich posiadania;
b) przeprowadzić kontrolę kompletności posiadanych kopii archiwalnych;
c) ustalić odpowiedzialność osób za powstanie sytuacji.

5. Sprawdzić nośniki, na których składowane są kopie archiwalne bazy danych. Usunąć przyczynę, która spowodowała powstanie podejrzenia naruszenia ochrony danych osobowych.

6. Jeżeli dane na dysku zostały uszkodzone lub zniszczone – odtworzyć je z kopii archiwalnej.

7. Sporządzić protokół dokonanych czynności.

8. Przeprowadzić szkolenie użytkowników w zakresie związanym z przetwarzaniem danych osobowych.

9. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy przejść do procedury opisanej w § 5.

§ 5

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

1. W sytuacji naruszenia ochrony danych osobowych należy powiadomić Dyrektora Ośrodka Miejskiego Ośrodka Pomocy Rodzinie oraz administratora bezpieczeństwa informacji o zaistniałej sytuacji.
2. Powiadomić Generalnego Inspektora Ochrony Danych Osobowych o zaistniałej sytuacji, a w przypadkach tego wymagających również Policję.
3. Zabezpieczyć dane, a w przypadkach tego wymagających również miejsce, pomieszczenia oraz inne ewentualne ślady.
4. Jeżeli jest to możliwe, przeciwdziałać rozpowszechnianiu zagrożonych danych.
5. Stosować się do poleceń Generalnego Inspektora Ochrony Danych Osobowych i/lub organów ścigania, a jeśli takich nie ma stosować procedury z § 4 odpowiednio.
6. Sporządzić protokół dokonanych czynności.