

# Instrukcja postępowania z incydentami bezpieczeństwa

Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.

## Opis zdarzeń naruszających ochronę danych osobowych.

Zdarzeniami naruszającymi ochronę danych osobowych bądź stwarzającymi podejrzenie naruszenia zabezpieczeń tych danych mogą być następujące przypadki:

* sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby bazy członkowskiej jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.,
* niewłaściwe parametry środowiska, takie jak np. nadmierna wilgotność, zbyt wysoka temperatura, oddziaływanie pola elektromagnetycznego,
* awaria sprzętu lub oprogramowania, które wyraźnie wskazują na celowe działanie   
  w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
* komunikaty alarmujące o próbie naruszenia zabezpieczeń bazy członkowskiej, który zapewnia ochronę danych bądź komunikat o podobnym znaczeniu,
* odstępstwa od prawidłowego stanu danych wskazujące na niewłaściwe działania bazy członkowskiej i niepożądaną jej modyfikację,
* naruszenie lub próba naruszenia integralności bazy członkowskiej,
* modyfikacja lub próba modyfikacji danych oraz zmiana w strukturze danych dokonana bez odpowiedniego upoważnienia (autoryzacji),
* stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w bazie członkowskiej,
* ujawnienie danych osobowych lub objętych tajemnicą procedur ochrony danych osobowych osobom nieupoważnionym, bądź innych elementów zabezpieczeń,
* funkcjonowanie bazy członkowskiej wykazuje nieprzypadkowe odstępstwo od prawidłowego rytmu pracy wskazujące na zaniechanie lub przełamanie ochrony danych osobowych lub np. pracę w bazie lub przy komputerze osoby do tego nieupoważnionej, sygnał o nieautoryzowanym logowaniu itp.,
* ujawnienie nieautoryzowanych kont dostępu do danych objętych ochroną,
* zniszczenie lub podmiana nośnika z danymi osobowymi bądź skasowanie lub skopiowanie danych osobowych w sposób niedozwolony lub przez osobę nieupoważnioną,
* rażące naruszenie dyscypliny w zakresie przestrzegania procedur bezpieczeństwa informacji np. niewylogowanie się z bazy członkowskiej, pozostawienie danych osobowych w drukarce, na ksero, niewykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych itp.,
* stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, płytach CD /DVD w formie niezabezpieczonej itp.

## Postępowanie w przypadku naruszenia danych osobowych.

### W przypadku stwierdzenia naruszenia ochrony danych osobowych, osoba odpowiedzialna za przewarzanie tych danych jest zobowiązana niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych lub Inspektora Danych Osobowych.

### Do czasu poinformowania Administratora Danych Osobowych lub Inspektora Danych Osobowych, należy:

#### niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,

#### rozważyć wstrzymanie bieżącej pracy na komputerze,

#### zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowania i analizę,

#### podjąć inne stosowne działania przewidziane w instrukcjach technicznych i technologicznych, dokumentacji bazy danych lub aplikacji użytkowej, właściwe dla objawów sytuacji towarzyszącej naruszeniu,

#### udokumentować wstępnie zaistniałe zdarzenie.

### Po poinformowaniu, Administrator Danych Osobowych lub Inspektor Danych Osobowych:

#### zapoznaje się z zaistniałą sytuacją, identyfikuje rodzaj zaistniałego zdarzenia, dokonuje wyboru metody dalszego postępowania celem powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych osobowych,

#### może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jakrównież innych osób mogących posiadać informacje związane z zaistniałym zdarzeniem.

#### podejmuje decyzje o konieczności zgłoszenia incydentu do organu nadzorczego.