Instrukcja
postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1

Niniejsza instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w Systemie Informatycznym. Instrukcję stosuje się w przypadku stwierdzenia naruszenia zabezpieczeń sprzętu informatycznego, sieci komputerowej lub zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

§ 2

1. Każda osoba zatrudniona przy przetwarzaniu danych osobowych, która stwierdzi lub podejrzewa naruszenie ochrony danych w Systemie Informatycznym, zobowiązana jest do niezwłocznego poinformowania o tym Inspektora Ochrony Danych lub w przypadku jego nieobecności bezpośredniego przełożonego.
2. Do czasu przybycia Inspektora Ochrony Danych na miejsce naruszenia ochrony danych osobowych, należy:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   d) podjąć inne działania, określone w instrukcjach technicznych i technologicznych, stosownie do objawów i komunikatów towarzyszących naruszeniu,
   e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   g) udokumentować wstępnie zaistniałe naruszenie,
   h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji.

§ 3

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Inspektor Ochrony Danych:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) jeżeli zasoby systemu na to pozwalają, generuje i drukuje wszystkie raporty, które mogą pomoc w ustaleniu wszelkich okoliczności zdarzenia,

4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych:
   a) fizycznie odłącza urządzenia i segmenty sieci, które mogłyby umożliwić dostęp do bazy danych osobie niepowołanej,
   b) wyloguje użytkownika podejrzanego o naruszenie ochrony danych,
   c) zmienia hasła konta administratora i użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.
2) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Inspektora Ochrony Danych,
3) jeżeli zachodzi taka potrzeba, nawiązuje kontakt z właściwymi specjalistami.

§ 4

1. Po wyczerpaniu niezbędnych środków doraźnych, Inspektora Ochrony Danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii bezpieczeństwa i terminu wznowienia przetwarzania danych.
2. Inspektora Ochrony Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,
   c) określenie okoliczności towarzyszących i rodzaju naruszenia,
   d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
3. Raport, o którym mowa w ust. 2 Inspektor Ochrony Danych przekazuje organowi nadrzędnemu (GIODO) w ciągu 72 godzin od wystąpienia.
4. Wzór raportu, o którym mowa w ust. 2 i 3 stanowi załącznik nr 2 do Polityki Bezpieczeństwa.
5. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę. w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.