

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. Instrukcja określa sposób postępowania w sytuacji naruszenia ochrony danych osobowych.
2. Przez użyte w Instrukcji pojęcia rozumie się:
 - a) *dane osobowe* – każda informacja dotycząca osoby fizycznej pozwalająca określić jej tożsamość,
 - b) *system informatyczny* – system sprzętowo - osobowy przetwarzający dane osobowe,
 - c) *administrator danych* – dyrektor szkoły,
 - d) *administrator bezpieczeństwa informacji* – osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym,
 - e) *administrator systemu* – osoba odpowiedzialna za sprawne funkcjonowanie systemu informatycznego,
 - f) *użytkownik* – osoba upoważniona do dostępu do danych osobowych,
 - g) *naruszenie ochrony danych osobowych* – sytuacja lub stan w którym dokonano naruszenia bezpieczeństwa danych,
 - h) *naruszenie zabezpieczenia systemu informatycznego* – jakiegokolwiek naruszenie bezpieczeństwa dokonane przez osoby niepowołane lub nieumyślnie.
3. Za naruszenie ochrony danych osobowych uznaje się przypadki:
 - a) stwierdzenie naruszenia zabezpieczenia danych w systemie informatycznym,
 - b) stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogące wskazywać na naruszenie zabezpieczeń tych danych.
2. Tabela form naruszeń bezpieczeństwa danych osobowych wraz z kodami zawiera załącznik nr 9.
3. Użytkownik, który stwierdził lub podejrzewa naruszenie danych osobowych jest zobowiązany do niezwłocznego powiadomienia o tym administratora danych, administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę.
4. Administrator bezpieczeństwa informacji, który stwierdził lub uzyskał informacje o naruszeniu bezpieczeństwa danych jest zobowiązany do niezwłocznego:
 - a) zapisania informacji i okoliczności związanych z tym zdarzeniem,
 - b) jeżeli możliwości systemu na to pozwalają, wygenerowanie lub wydrukowanie wszystkich dokumentów, które mogą pomóc w ustaleniu wszystkich okoliczności zdarzenia,
 - c) przystąpienia do oceny skali zniszczeń, techniki naruszenia itp.,
 - d) podjęcia kroków celem uniemożliwienia dalszego naruszenia danych osobowych a w szczególności:
 - fizycznego odłączenia urządzeń i sieci,
 - wylogowania użytkownika podejrzanego o naruszenie ochrony,
 - zmiana hasła administratora lub użytkownika, z których uzyskano nielegalny dostęp do danych,
 - e) szczegółowej analizie stanu systemu informatycznego celem potwierdzenia lub wykluczenia naruszenia ochrony danych osobowych,
 - f) przywrócenia normalnego działania systemu włącznie z odtworzeniem uszkodzonych danych z kopii bezpieczeństwa,
 - g) sporządza raport z sytuacji naruszenia bezpieczeństwa danych osobowych będący załącznikiem nr 10.

4. Po przywróceniu normalnego funkcjonowania systemu informatycznego należy podjąć działania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. A w szczególności:
 - a) jeżeli przyczyną zdarzenia był błąd użytkownika należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych,
 - b) jeżeli przyczyną była infekcja wirusowa należy ustalić źródło i wykonać zabezpieczenie systemowe i organizacyjne,
 - c) jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy u ustawy o ochronie danych osobowych.
5. Administrator bezpieczeństwa informacji przygotowuje szczegółowy raport o naruszeniu będący załącznikiem nr 11 w terminie 14 dni od daty jego zaistnienia i niezwłocznie przedstawia go administratorowi danych.