**XII. PROCEDURA POSTĘPOWANIA**

**W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH w Przedszkolu Miejskim nr 8 w Pabianicach**

**Podstawa prawna:**

* rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

**1. Cele postępowania w przypadku naruszenia ochrony danych osobowych**

Procedura została opracowana w celu ustalenia postępowania w przypadku naruszenia ochrony danych osobowych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,

- nieautoryzowane modyfikacje lub zniszczenie danych,

- udostępnienie danych nieautoryzowanym podmiotom,

- nielegalne ujawnienie danych,

- pozyskiwanie danych z nielegalnych źródeł.

**2. Procedura postępowania w przypadku naruszenia danych osobowych**

2.1 Zgłaszanie naruszeń ochrony danych osobowych

2.1.1 Każdy kto podejrzewa lub stwierdzi naruszenie ochrony danych osobowych, ma obowiązek niezwłocznie:

a) powiadomić o zaistniałym zdarzeniu dyrektora przedszkola,

b) Dyrektor przedszkola zgłasza zaistniały fakt Inspektorowi Ochrony Danych.

2.1.2 Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:

a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,

b) dokumentacja jest niszczona w sposób umożliwiający identyfikację ,

c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,

d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

e) nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,

f) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,

g) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia,

h) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,

i) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji); j. telefoniczne próby wyłudzenia danych osobowych,

j) kradzież komputerów lub twardych dysków z danymi osobowymi,

k) utrata kontroli nad kopią danych osobowych,

l) maile zachęcające do ujawnienia identyfikatora i/lub hasła,

ł) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,

m) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki",

n) hasła do systemów przechowywane są w pobliżu komputera.

2.1.3 Powiadomienie o podejrzeniu naruszenia ochrony danych osobowych należy przesłać za pośrednictwem służbowej poczty elektronicznej na adres mailowy lub przekazać telefonicznie lub osobiście Inspektorowi Ochrony Danych, jeżeli naruszenie miało związek z przetwarzaniem danych w systemach informatycznych.

2.1.4 Powiadomienie, o którym mowa w pkt 2.1.2, powinno zawierać precyzyjne i wyczerpujące informacje, określające:

a) czas, miejsce i okoliczności zdarzenia,

b) symptomy świadczące o możliwości naruszenia ochrony danych osobowych,

c) inne okoliczności i fakty mogące pomóc w ustaleniu przyczyn naruszenia zasad ochrony danych osobowych.

2.1.5 Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

2.1.6 W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub innej osoby upoważnionej przez Administratora danych.

2.1.7 Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.

**2.2 Postępowanie wyjaśniające**

2.2.1 Postępowania wyjaśniające w sprawach dotyczących naruszenia ochrony danych osobowych w Przedszkolu Nr 8 prowadzi Inspektor Ochrony Danych.

2.2.2 Po otrzymaniu powiadomienia, o którym mowa w pkt 2.1.2, Inspektor Ochrony Danych ocenia sytuację i podejmuje poniższe działania:

1) dokonuje rozpoznania zdarzenia;

2) lokalizuje źródło problemu;

3) ocenia wagę problemu;

4) określa środki mające na celu likwidację skutków naruszenia oraz zapobiegawcze, chroniące przed wystąpieniem podobnego zdarzenia w przyszłości.

2.2.3 W sytuacji naruszenia ochrony przetwarzania danych osobowych w systemie informatycznym, Inspektor Ochrony Danych wyjaśnia zdarzenie we współpracy z Informatykiem, ocenia sytuację i podejmuje odpowiednie do potrzeb działania, określone w pkt 2.1.6.

2.2.4 Każdy zidentyfikowany incydent, naruszający ochronę danych osobowych, musi być rozpoznany i wyjaśniony w ciągu 24 godzin od momentu otrzymania zgłoszenia o jego wystąpieniu.

2.2.5 Każde postępowanie wyjaśniające kończy się analizą skutków naruszenia i sporządzeniem raportu, zawierającego podjęte działania naprawcze oraz wnioski dotyczące w szczególności proponowanych działań zapobiegawczych, a także informację o konieczności podjęcia działań, o których mowa w pkt 3.2. lub 3.3 oraz 3.4.

2.2.6 Raport, podpisany przez Inspektora Ochrony Danych przekazywany jest niezwłocznie Dyrektorowi Przedszkola.

2.2.7 Inspektor Ochrony Danych, stosownie do postanowień zawartych w art. 33 ust. 5, dokumentuje wszelkie naruszenia ochrony danych osobowych, w formie rejestru zgłoszonych incydentów.

2.2.8 Inspektor Ochrony Danych ma obowiązek niezwłocznego przedstawienia zebranych materiałów administratorowi danych, który z pomocą inspektora , w terminie i na podstawie przesłanek określonych w ogólnym rozporządzeniu o ochronie danych powinien ocenić, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu.

 2.2.9 Jeżeli istnieje taki obowiązek – sporządzenie zgłoszenia do organu nadzorczego oraz zamieszczeniu informacji naruszeniu na stronie www lub BIP jednostki.