Zarządzenie nr 8/2020/2021
dyrektora Zespołu Szkolno-Przedszkolnego nr 15 w Rybniku
z dnia 7 października 2020 roku

w sprawie: **wprowadzenia „Procedury zarządzania ryzykiem naruszenia praw lub wolności osób fizycznych" oraz zmiany „Procedury zarządzania ryzykiem w bezpieczeństwie informacji"**

Działając na podstawie:

- art. 24, 25 i 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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),
- § 20 ust. 1 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

zarządzam, co następuje:

§ 1.

Wprowadzam „Procedurę zarządzania ryzykiem naruszenia praw lub wolności osób fizycznych", która stanowi załącznik do zarządzenia.

§ 2.

§ 1 „Procedury zarządzania ryzykiem w bezpieczeństwie informacji" otrzymuje brzmienie:

1. *„Procedura zarządzania ryzykiem w bezpieczeństwie informacji", zwana w dalszej części* „Procedurą", określa zasady przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, w Zespole Szkolno-Przedszkolnym nr 15 w Rybniku.
2. Ilekroć w *„Procedurze" jest mowa o:*
   1) *dyrektorze* – należy przez to rozumieć dyrektora Zespołu Szkolno-Przedszkolnego nr 15 w Rybniku lub osobę zastępującą,
   2) *ryzyku* – należy przez to rozumieć ryzyko w bezpieczeństwie informacji,
   3) *Zespole* – należy przez to rozumieć Zespół Szkolno-Przedszkolny nr 15 w Rybniku.

§ 3.

Nadzór nad realizacją zarządzenia sprawuje dyrektor.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do zarządzenia nr 8/2020/2021 – „*Procedura zarządzania ryzykiem naruszenia praw lub wolności osób fizycznych”*

PROCEDURA ZARZĄDZANIA RYZYKIEM NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

§ 1.

„Procedura zarządzania ryzykiem naruszenia praw lub wolności osób fizycznych”, zwana w dalszej części „Procedurą”, określa zasady przeprowadzania okresowych analiz ryzyka naruszenia praw i wolności osoby, której dane dotyczą oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, w Zespole Szkolno-Przedszkolnym nr 15 w Rybniku, zwanym w dalszej części „Procedury” Zespołem.

§ 2.

1. Ryzyko to wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Ryzyko jest proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.
2. Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania Zespołu w odniesieniu do ryzyka. W ramach zarządzania ryzykiem analizuje się, co może się zdarzyć i jakie mogą być możliwe następstwa, a następnie podejmuje decyzję, co i kiedy należy wykonać, aby zredukować ryzyko do akceptowalnego poziomu.

§ 3.

1. Prawdopodobieństwo ryzyka jest to oczekiwana częstotliwość wystąpienia zdarzenia zdefiniowanego jako ryzyko.
2. Strata, którą może spowodować ryzyko jest to wpływ zdarzenia zdefiniowanego jako ryzyko na osoby fizyczne w przypadku naruszenia ich praw i wolności.

§ 4.

1. Ocena ryzyka polega na określeniu prawdopodobieństwa ryzyka i straty, którą może spowodować ryzyko.
2. Oceny ryzyka dokonuje się poprzez przyznanie prawdopodobieństwu ryzyka i stracie, którą może spowodować ryzyko odpowiedniej liczby punktów.
3. Punktacja dla prawdopodobieństwa ryzyka:
   1) prawie pewne – 3 pkt,
   2) możliwe – 2 pkt,
   3) rzadkie – 1 pkt.
4. Punktacja dla straty, którą może spowodować ryzyko:
   1) naruszenie z bardzo dużym prawdopodobieństwem może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną – 3 pkt,
   2) naruszenie w zależności od kontekstu danego zdarzenia w niektórych przypadkach może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną – 2 pkt,

3) naruszenie nie będzie wpływało na prawa i wolności osób fizycznych – 1 pkt.

5. Oceny ryzyka występujące w Zespole:
   a) ryzyko wysokie – suma przyznanych punktów od 5 do 6. Duża istotność. Konsekwencje poważne. Niezbędne są działania naprawcze,
   b) ryzyko średnie – suma przyznanych punktów od 3 do 4. Średnia istotność. Przeciwdziałanie wskazane,
   c) ryzyko niskie – suma przyznanych punktów od 1 do 2. Mała istotność. Przeciwdziałanie zależy od decyzji właściciela ryzyka.

§ 5.

1. W przypadku ryzyka wysokiego lub średniego konieczne jest postępowanie z ryzykiem.
2. Metody postępowania z ryzykiem występujące w Zespole:
   a) unikanie – eliminacja zagrożeń,
   b) przeniesienie – przeniesienie ryzyka na inny podmiot, np. poprzez outsourcing lub ubezpieczenie,
   c) łagodzenie – podjęcie działań mających na celu zmniejszenie negatywnych skutków wystąpienia zagrożenia,
   d) akceptacja – zaakceptowanie istniejącego ryzyka i wstrzymanie reakcji do chwili zaistnienia zagrożenia.
3. Postępowanie z ryzykiem powinno być proporcjonalne do ryzyka tak, aby, w większości przypadków, ryzyko mieć pod kontrolą, a nie je eliminować.
4. Postępując z ryzykiem należy brać pod uwagę w szczególności:
   1) ograniczenia czasowe (zabezpieczenie powinno zostać wdrożone w czasie „życia" danych osobowych lub systemu),
   2) ograniczenia finansowe (zabezpieczenia nie powinny być bardziej kosztowne do wdrożenia lub utrzymania niż strata, którą może przynieść ryzyko, za wyjątkiem sytuacji, gdy osiągnięcie zgodności jest wymagane przepisami prawa),
   3) ograniczenia techniczne,
   4) ograniczenia kulturowe (jeśli pracownicy nie rozumieją zabezpieczenia lub nie akceptują go, to zabezpieczenie staje się z czasem nieskuteczne),
   5) ograniczenia prawne,
   6) łatwość użycia,
   7) ograniczenia przy integrowaniu nowych i istniejących zabezpieczeń.

§ 6.

1. Oceny ryzyka dokonuje dyrektor, inspektor ochrony danych, a także – w razie potrzeby – inni pracownicy Zespołu wyznaczeni przez dyrektora.
2. Ocenę ryzyka należy udokumentować.

§ 7.

W sprawach nieuregulowanych w „Procedurze" decyzję podejmuje dyrektor.