PROCEDURA DZIAŁANIA NA WYPADEK INCYDENTU W OBSZARZE OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKOLNO – PRZEDSZKOLNYM NR 17 WE WROCŁAWIU

Incydent – sytuacja lub zdarzenie, które wiąże się z co najmniej jednym z następujących skutków:

a) bezpowrotna utrata danych osobowych (np. zniszczenie dysku, który nie ma kopii zapasowej)
b) wyciek danych osobowych (uzyskanie dostępu do danych osobowych przez osobę nieuprawnioną)
c) naruszenie integralności danych (doszło do nieautoryzowanych zmian w bazach danych, które np. skutkują brakiem możliwości stwierdzenia prawidłowości danych).

W przypadku podejrzenia wystąpienia incydentu przyjmuje się następujące reguły działania:

Krok 1 – pracownik, który stwierdzi ryzyko incydentu, niezwłocznie zabezpiecza dane przed dalszym wyciekiem/zniszczeniem przy jednoczesnym zachowaniu danych dot. **zdarzenia** (tj. należy zabezpieczyć dane przed dalszym dostępem osób nieuprawnionych, a jednocześnie należy zachować informacje o tym jakie dane wyciekły, w celu umożliwienia działania w kolejnych krokach; przykładowo w przypadku włamania na serwer jednostki i wykradzenia danych, odłączamy serwer od Internetu ale nie kasujemy danych zawartych na serwerze – będą potrzebne do zidentyfikowania jaka była skala naruszenia i jakie dane zostały narażone)

Krok 2 – pracownik, który stwierdził ryzyko incydentu, po wykonaniu działań z kroku 1 niezwłocznie informuje przełożonego oraz inspektora ochrony danych osobowych tomasz.grzybowski@coreconsulting.pl o zdarzeniu.

Krok 3 – Inspektor Ochrony Danych we współpracy z Dyrkecją placówki oraz zazwyczaj z osobą odpowiedzialną za systemy IT dokonują wtórnej weryfikacji bezpieczeństwa danych osobowych

Krok 4 – zostaje powołana wewnętrzna Komisja w celu zbadania okoliczności sprawy i określenie jej przebiegu, przyczyn naruszenia, potencjalnych konsekwencji naruszenia

Krok 5 – następuje podjęcie decyzji o konieczności zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych oraz osób, których dane dotyczą o wystąpieniu naruszenia

***Krok 6** – zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o incydencie (jeżeli są spełnione warunki z art. 33 RODO; wzór zgłoszenia stanowi Załącznik nr 1 do procedury

Krok 7 – opracowanie pełnego Raportu ze zdarzenia; wyciągnięcie określonych wniosków w zakresie koniecznych zmian proceduralnych, zabezpieczeń fizycznych lub technicznych; konsekwencji personalnych (jeżeli dotyczy); wpisanie incydentu do rejestru naruszeń

UWAGA: zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o naruszeniach, które wiążą się z istotnym ryzykiem naruszenia praw lub wolności osób, których dane dotyczą powinno być dokonane niezwłocznie, nie później jednak niż w terminie **72 godzin** po stwierdzeniu naruszenia. Nie są to „godziny robocze", więc działania w tym obszarze powinny być podejmowane bez zbędnej zwłoki.

Załączniki:

1. Wzór formularza zgłoszenia naruszenia
2. Rejestr naruszeń
3. Formularz potwierdzający zapoznanie się z Procedurą na wypadek incydentu bezpieczeństwa (dla pracowników, którzy nie posiadają adresu e-mail).