**Załącznik nr 7**

**do ZARZĄDZENIA NR 5**

**Przewodniczącego Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności w Świebodzinie**

**z dnia 24 maja 2018 r.**

**PROCEDURA DZIAŁANIA NA WYPADEK INCYDENTU**

**W OBSZARZE OCHRONY DANYCH OSOBOWYCH**

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

1. bezpowrotna utrata danych osobowych (np. zniszczenie dysku, który nie ma kopii zapasowej)
2. wyciek danych osobowych (uzyskanie dostępu do danych osobowych przez osobę nieuprawnioną)
3. 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. przykładowo należy zabezpieczyć dostęp do danych przez osoby nieuprawnione, a jednocześnie należy zachować informacje o tym jakie dane wyciekły, w celu umożliwienia działania w kolejnych krokach)

**Krok 2** – pracownik, który stwierdził ryzyko incydentu, po wykonaniu działań z kroku 1 niezwłocznie informuje przełożonego oraz Inspektora Ochrony Danych Osobowych o zdarzeniu

**Krok 3** – Inspektor we współpracy z Przewodniczącym Zespołu oraz zazwyczaj z osobą odpowiedzialną obsługę informatyczną urzędu 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** – 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 zgłoszenie 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)

**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.