Szacowanie ryzyka - schemat postępowania wg PN- ISO/IEC 27005

1. Określ kontekst
2. Zidentyfikuj ryzyka
   - 2.1 Zidentyfikuj aktywa
   - 2.2 Zidentyfikuj zagrożenia
   - 2.3 Zidentyfikuj istniejące zabezpieczenia
   - 2.4 Zidentyfikuj podatności
   - 2.5 Zidentyfikuj następstwa
3. Dokonaj analizy ryzyka
   - 3.1 Oszacuj następstwa (przypisz wartość)
   - 3.2 Oszacuj prawdopodobieństwo incydentu (przypisz wartość)
   - 3.3 Określ poziom ryzyka
4. Oceń ryzyko
5. Wybierz sposób postępowania z ryzykiem

- Przykładowy zakres dokumentu polityki:
  - Ogólne zasady ochrony danych
  - Zakres odpowiedzialności osób zarządzających
    - Zarząd oraz kierownicy komórek organizacyjnych
  - Zakres odpowiedzialności Inspektora ochrony danych
  - Zakres odpowiedzialności osób upoważnionych do przetwarzania danych
  - Zasady upoważniania osób do przetwarzania danych osobowych
  - Zasady prowadzenia rejestrów czynności przetwarzania danych osobowych

- Zasady realizacji obowiązków przy przetwarzaniu danych osobowych, w tym:
  - Zapewnienia podstaw prawnych dla przetwarzania danych, w tym ich udostępniania innym podmiotom
  - Realizacji obowiązku informacyjnego przy zbieraniu danych
  - Realizacji obowiązków przy powierzaniu przetwarzania danych
  - Realizacji obowiązków przy transferze danych do państwa trzeciego lub organizacji międzynarodowej
  - Realizacji obowiązków dotyczących retencji danych
- Zasady realizacji praw osób, których dane dotyczą

- Zasady doboru środków technicznych i organizacyjnych dotyczących przetwarzania i zabezpieczania danych osobowych, w tym określenie procedur:
  - szacowania ryzyka naruszenia praw i wolności osób, których dane dotyczą
  - uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych
  - dokonywania oceny skutków dla ochrony danych
- Zasady postępowania w sytuacji naruszenia ochrony danych
- Zasady rozliczalności zgodności realizacji obowiązków RODO
- Odpowiedzialność karna za naruszenie zasad ochrony danych