

# Program szkolenia

## Ochrona danych osobowych

### 1. Wstęp – przedstawienie się.

### 2. Ochrona danych osobowych wg obowiązujących przepisów.

- ochrona danych osobowych w systemie prawa polskiego;
- zasady przetwarzania danych osobowych;
- zakres podmiotowy i przedmiotowy ustawy o ochronie danych osobowych;
- omówienie odpowiedzialności osób przetwarzających dane osobowe, w tym roli Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych;
- prawa osób, których dane dotyczą;
- zabezpieczenie danych osobowych przetwarzanych w formie manualnej (papierowej) oraz elektronicznej;
- odpowiedzialność za naruszenie zasad dotyczących danych osobowych;
- działalność GIODO – jego zakres działania, funkcje oraz kompetencje;
- rejestrowanie zbiorów danych osobowych oraz osób pełniących funkcję ABI u Generalnego Inspektora Ochrony Danych Osobowych (GIODO)

### 3. Reforma przepisów o ochronie danych osobowych i ich wejście w życie z dniem 25 maja 2018 roku – omówienie najważniejszych zmian w przepisach.

- bezpośrednia odpowiedzialność podmiotów przetwarzających dane;
- zgłaszanie naruszeń oraz incydentów;
- nowe i rozszerzone prawa obywateli;
- wyznaczenie Inspektora Ochrony Danych Osobowych;
- obowiązkowa inwentaryzacja danych i wymagania związane z dokumentacją;
- zgody;
- rozbudowanie obowiązku informacyjnego;
- ocena wpływu ochrony danych;
- transfer danych poza Unię Europejską.

### 4. Wdrożenie zapisów RODO w praktyce – omówienie.

- pojęcie RODO lub GDPR?;
  - nowe Rozporządzenie a Ustawa o ochronie danych osobowych;
  - czas i zakres zastosowania RODO;
  - zasady przetwarzania danych osobowych – co przewiduje RODO?;
  - ochrona osób fizycznych;
  - pojęcie anonimizacji i pseudonimizacji;
  - profilowanie – omówienie zagadnienia;
  - Privacy by design oraz privacy by default;
  - Privacy Shield – podstawowe obowiązki administratorów i podmiotów przetwarzających;
  - uprawnienia organów nadzorczych, skargi i sankcje.
-

## Program szkolenia

### 5. Rozporządzenie RODO a szyfrowanie danych – omówienie.

- Wdrożenie środków technicznych i organizacyjnych (w tym pseudonimizacji i szyfrowania danych osobowych).

### 6. Bezpieczne użytkowanie sprzętu teleinformatycznego, za pomocą którego przetwarza się dane osobowe. Wprowadzenie procedur zabezpieczających sprzęt IT przed utratą danych – omówienie.

- czym jest bezpieczeństwo teleinformatyczne?
- wprowadzenie procedur bezpieczeństwa sieciowego;
- szyfrowanie danych oraz nośników pamięci;
- zabezpieczanie poczty e-mail;
- serwisowanie sprzętu IT przetwarzającego dane osobowe.

### 7. Realizacja czynności audytowych przeprowadzanych przez Administratora Bezpieczeństwa Informacji (później Inspektora Ochrony Danych Osobowych) w podmiotach publicznych i prywatnych przetwarzających dane osobowe.

- analiza posiadanych procedur ochrony danych osobowych (polityki, instrukcji, załączników) pod kątem jej zgodności z obowiązującymi przepisami prawa;
  - przesłanki legalności przetwarzania danych osobowych zwykłych i wrażliwych;
  - sprawdzenie zakresu oraz celu przetwarzania danych osobowych;
  - weryfikacja systemu techniczno – organizacyjnego ochrony danych osobowych;
  - sprawdzenie zabezpieczeń i konfiguracji infrastruktury informatycznej;
  - sprawdzenie poziomu zabezpieczeń zbiorów danych osobowych przetwarzanych w formie manualnej (papierowej);
  - weryfikacja zawartych umów handlowo-usługowych i cywilnoprawnych pod kątem ich zgodności z obowiązującymi przepisami prawa;
  - sprawdzenie umów dotyczących powierzenia przetwarzania danych osobowych.
-