# Program szkolenia

**1**

**BLOK TEMATYCZNY**
**09:00-10:30**

### Wstęp

- Unijne Rozporządzenie o ochronie danych osobowych: zakres stosowania.
- Administrator Danych – obowiązki, prawa, odpowiedzialność.
- Inspektor Ochrony Danych Osobowych (IOD) – rola, obowiązki, umiejscowienie w systemie ochrony danych wew. organizacji – pierwsze doświadczenia.
- Dotychczasowe doświadczenia z funkcjonowania RODO.
- Kierunki zmian w przepisach.
- Najnowsze wytyczne Prezesa Urzędu Ochrony Danych.
- Rządowy projekt przepisów wdrażających RODO do polskiego porządku prawnego.

**10:30-10:45**

### Przerwa kawowa

**2**

**BLOK TEMATYCZNY**
**10:45-12:30**

### Część I – Ochrona danych osobowych w organizacji w kontekście zmian w przepisach

- Jakie dane można przetwarzać w organizacji: rodzaje, kategorie, zgody.
- Obowiązek informacyjny w obszarach procesów administracyjnych, kadr, działań marketingowych, sposobów komunikacji, profilowania.
- Korzystanie z usług firm zewnętrznych w kontekście powierzenia danych osobowych.
- Monitoring w organizacji – zasady monitoringu wizyjnego, elektronicznego, obowiązek informacyjny.
- Metodologia sporządzania dokumentacji bezpieczeństwa przetwarzania danych osobowych.
- Szacowanie ryzyka w zakresie przetwarzania danych.
- osobowych w instytucji – studium przypadków.

# Program szkolenia

**12:30-13:00**

**Otwarta dyskusja, podczas której przedstawiciele administracji publicznej będą mogli podzielić się swoimi doświadczeniami dotyczącymi praktyki stosowania nowych przepisów.**

**13:00-13:30**

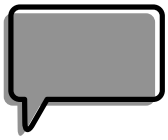
## Lunch

**3**

**BLOK TEMATYCZNY**
**13:30-15:00**

**Część II – Zarządzanie bezpieczeństwem i weryfikacja zabezpieczeń.**

- RODO, a funkcjonowanie systemów IT działających w administracji publicznej.
- RODO, a systemy działające w Urzędach. Odpowiedzialność za ich dostosowanie do wymogów RODO – stan obecny.
- Klasyfikacja zasobów danych osobowych (co podlega inwentaryzacji i do czego jest ona potrzebna?) – studium przypadków.
- Zagrożenia bezpieczeństwa w administracji.
- Zabezpieczenia techniczne i organizacyjne – dobre praktyki bezpieczeństwa, zalecenia i wytyczne grupy roboczej art.29.
- Analiza ryzyka bezpieczeństwa przetwarzania danych osobowych – praktyczne podejście do DPIA, wymagane dokumenty, sposób realizacji.
- Wyniki przeprowadzonych kontroli.
- Ochrona danych wrażliwych – doświadczenia i praktyka.
- Audytowanie procesów w organizacji pod kątem bezpieczeństwa danych osobowych – postępowanie w przypadku naruszenia prywatności w procesie przetwarzania danych osobowych.



**15:00-15:15**

## Podsumowanie, dyskusja