

Rola Inspektora Ochrony Danych Osobowych w przedsiębiorstwie wod-kan.

Warsztaty prawno-techniczne

Kraków, 14-15 lutego 2019 r., Sopot, 25-26 kwietnia 2019 r.

Dzień I. Zagadnienia prawne

1) Inspektor ochrony danych w przepisach prawa:

- Zakres podmiotowy obowiązku powołania inspektora ochrony danych
- Kto może być inspektorem ochrony danych?
- Zgłaszania inspektora ochrony danych
- Status inspektora ochrony danych w przedsiębiorstwie wodociągowym

2) Zadania inspektora ochrony danych:

- Informowanie przedsiębiorstwa wodociągowego o obowiązkach wynikających z przepisów prawa. Zasada rozliczalności w praktyce
- Informowanie podmiotu przetwarzającego o obowiązkach wynikających z przepisów prawa. Powierzenie a udostępnienie. Aspekty praktyczne
- Informowanie pracowników o obowiązkach wynikających z przepisów prawa. Zakładowe źródła prawa pracy a podstawa przetwarzania danych osobowych. Aspekty praktyczne
- Doradzanie w procesie ochrony danych osobowych. Aspekty praktyczne stosowania RODO
- Jak monitorować przestrzeganie RODO i polityk ochrony danych osobowych?
- Podział obowiązków i działania zwiększające świadomość
- Szkolenie personelu uczestniczącego w operacjach przetwarzania
- Audyty – część prawna
- Współpraca z organem nadzorczym
- Punkt kontaktowy dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach

Dzień II. Zagadnienia techniczne

1) Wymagania techniczne wynikające z RODO

- Rejestry czynności przetwarzania I kategorii przetwarzania
- Obowiązki względem osób, których dane są przetwarzane
- Procedury wynikające pośrednio z wymogów RODO

2) Ocena ryzyka – Data Protection Impact Analysis (DPIA)

- Kiedy DPIA jest wymagane
- Inwentaryzacja przepływów danych osobowych
- Wstępna DPIA
- Jak przeprowadzić DPIA dla wybranych procesów
- Raportowanie wyników DPIA

3) Nadzór and procesorami

- Umowy z procesorami, w tym umowa powierzenia przetwarzania danych osobowych
- Obsługa incydentów
- Audyty procesorów

4) „Privacy by design” i „Privacy by default”

5) Anonimizacja i Pseudonimizacja danych osobowych

6) Szkolenie personelu uczestniczącego w operacjach przetwarzania z ochrony danych osobowych

7) Wymagania dyrektywy NIS i Ustawy o krajowym systemie cyberbezpieczeństwa

- Zarządzanie incydentami bezpieczeństwa, w tym incydentami bezpieczeństwa danych osobowych, wraz z przekazywaniem do CSIRT
- Zgodność z ISO27001 w zakresie bezpieczeństwa danych osobowych i jak to powinno być zapewnione, w tym audyty bezpieczeństwa informacji
- Zgodność z ISO22301 – zapewnienie ciągłości działania

8) Monitorowanie działań naprawczych i raportowanie