# Zapraszamy na szkolenie dwudniowe:

# INSPEKTOR OCHRONY DANYCH - najnowsze przepisy, - szkolenie obejmuje autorskie warsztaty Case Study związane z analizą ryzyka. 14-15.03.2019 r. KATOWICE

CENA w przypadku zgłoszenia jednej osoby: 949 zł/netto.

**DZIEŃ I (7 h)**

1. **PRZED CZYM SIĘ CHRONIĆ - KRÓTKIE OMÓWIENIE ZAGROŻEŃ, PODATNOŚCI, INCYDENTÓW ORAZ TECHNIKI KRADZIEŻY DANYCH:**
2. statystyki wycieków danych,
3. konsekwencje wycieków danych,
4. przykłady handlu danymi w Polsce,
5. wartość danych.
6. **PRZEPISY SZCZEGÓŁOWE PRAWA POLSKIEGO:**
7. Kodeks pracy - uregulowania kodeksu w sprawie przetwarzania danych osobowych pracowników.
8. Przepisy BHP- dokumentacja powypadkowa, a ochrona danych.
9. Prawo Autorskie – wizerunek jako dana/informacja, manipulacja wizerunkiem.
10. Prawo Cywilne – dane osobowe jako dobro.
11. Kodeks karny - przepisy karne związane z bezpieczeństwem informacji.
12. Ustawa o świadczeniu usług drogą elektroniczną- adres e-mail jako dana osobowa.
13. **PRZEPISY O OCHRONIE DANYCH OSOBOWYCH:**
14. **nowelizacja przepisów o ochronie danych osobowych- omówienie podstawowych zmian spójnego Prawa Unijnego dotyczącego Ochrony Danych Osobowych z maja 2018 r.,** 
    * **wykaz różnić w odniesieniu do aktualnych przepisów,**
    * **nowe pojęcia i obowiązki w szczególności: profilowanie, prawo do przenoszenia danych, nowy obowiązek informacyjny wraz z nowymi zasadami pierwszego kontaktu z podmiotem danych, zasada „przejrzystości”, prawo do bycia zapomnianym.**
    * **Nowe podejście do ochrony danych.**
15. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.**:**

* „Rejestr Inspektorów Ochrony Danych” - kto może zostać IOD-em, jak zgłosić IOD-a, kto prowadzi rejestr i w jakiej formie,
* Zasady tworzenia sprawozdań dla Administratora Danych raportowania incydentów do PUOD,
* pozycja Inspektora Ochrony Danych;

1. **Nowe ustawowe obowiązki Inspektora Ochrony Danych w odniesieniu do Administratora Bezpieczeństwa Informacji:**
   * **Kto może, a kto nie może być IOD?**
   * **Podstawowe zadania IOD,**
   * **Prowadzenie rejestru czynności przetwarzania w porównaniu z jawnym wykazem zbiorów danych,**
   * **Plan sprawozdań- zostawić czy zrezygnować,**
   * **Pouczanie i upominanie osób niestosujących się do Polityki bezpieczeństwa.**
   * **Jak w praktyce wygląda praca IOD.**
2. **pojęcie danych osobowych oraz kategorii danych ze szczególnym naciskiem na tzw. „dane wrażliwe” / dane szczególnej kategorii np. stan zdrowia,**
3. Prezes Urzędu Ochrony Danych Osobowych- obowiązki i prawa,
4. szczegółowe omówienie pojęcia Administrator Danych Osobowych,
5. pozostałe podstawowe pojęcia ustawy o ochronie danych osobowych i RODO,
6. obowiązki związane z przetwarzaniem danych osobowych:

* legalne przetwarzanie danych osobowych,
* obowiązki informacyjne związane z przetwarzaniem danych osobowych ,
* podstawowe prawa i wolności osób fizycznych.

1. Powierzenie danych osobowych do przetwarzania- **zawieranie umów powierzenia danych osobowych do przetwarzania, przykłady umów powierzenia na nowych zasadach,**
2. przekazywanie danych osobowych za granice,
3. przepisy karne ustawy o ochronie danych osobowych.
4. **Panel dyskusyjny.**

**DZIEŃ II (7h)**

**1. PROCES ANALIZY RYZYKA, JAKIM POWINNY ODPOWIADAĆ URZĄDZENIA I SYSTEMY INFORMATYCZNE SŁUŻĄCE DO PRZETWARZANIA DANYCH OSOBOWYCH:**

1. „Niepotrzebny dokument?”- szczegółowe omówienie wytycznych co do formy i zawartości dokumentów Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,
2. osoby odpowiedzialne za opracowanie, wdrożenie i aktualizacje dokumentacji Polityki Bezpieczeństwa,
3. regulamin korzystania z sieci oraz infrastruktury IT,
4. wymogi bezpieczeństwa dotyczące pomieszczeń przetwarzania danych osobowych,
5. zabezpieczenia kryptograficzne przetwarzanych danych osobowych – omówienie narzędzi służących do szyfrowania,
6. przechowywanie i archiwizowanie danych osobowych,
7. zagrożenia płynące z sieci Internet - sposoby bezpiecznego korzystania z serwisów www, poczta elektroniczna - zasady bezpiecznej korespondencji,
8. praktyczne rozwiązania w zakresie opracowania i wdrożenia Polityki Bezpieczeństwa Informacji,
9. praktyczne rozwiązania w zakresie opracowania i wdrożenia Instrukcji Zarządzania Systemem Informatycznym,
10. Audyt- zaplanowanie, przeprowadzanie, wdrożenie działań korygujących.

**2. ĆWICZENIA- w tym analiza ryzyka.**

Ćwiczenia prowadzone są w formie Case Study. Ćwiczenia są zbudowane w taki sposób aby tworzyły całość podejścia do zagadnienia Polityki Bezpieczeństwa i związanymi z nią procedurami **opartymi na** **Szacowaniu Ryzyka.** Ćwiczenia są autorskim indywidualnym projektem (autor Michał Geilke), pokazują cztery najważniejsze Etapy wdrażania Polityki Bezpieczeństwa oraz najczęstsze problemy. Ćwiczenia obejmują szerokie spektrum zagadnień – od treści procedur i ich podstawy prawnej po elementy związane z identyfikacją zagrożeń oraz ich minimalizowaniem. **Ćwiczenia obejmują:**

1. Wdrożenie Polityki Bezpieczeństwa oraz powołanie Inspektora Ochrony Danych:
   * **Szacowanie ryzyka,**
   * **Reagowanie na ryzyko,**
   * **Zarządzanie ryzykiem.**
2. Nadawanie, modyfikacja i odbieranie upoważnienia do przetwarzania danych osobowych (zgodne z RODO).
3. Zbiory Danych osobowych i czynności przetwarzania:
   * identyfikacja zbiorów i ich elementów,
   * legalizacja elementów zbiorów,
   * identyfikacja zbiorów powierzonych lub otrzymanych w powierzeniu.
4. Procedury rozpoczęcia i zakończenia pracy z systemem informatycznym.
5. Legalne źródła danych.
6. Umowy powierzenia.
7. Raportowanie incydentów do Prezesa Urzędu Ochrony Danych Osobowych.
8. Raport z incydentu i Audyt – z punktu widzenia użytkownika oraz z punktu widzenia IOD.

**3. Panel dyskusyjny.**