

Zapraszamy na szkolenie dwudniowe:

INSPEKTOR OCHRONY DANYCH

- najnowsze przepisy,
- szkolenie obejmuje autorskie warsztaty Case Study związane z analizą ryzyka.

24-25.09.2018 r.

KATOWICE

DZIEŃ I (7 h)

1. PRZED CZYM SIĘ CHRONIĆ - KRÓTKIE OMÓWIENIE ZAGROŻEŃ, PODATNOŚCI, INCYDENTÓW ORAZ TECHNIKI KRADZIEŻY DANYCH:

- a) statystyki wycieków danych,
- b) konsekwencje wycieków danych,
- c) przykłady handlu danymi w Polsce,
- d) wartość danych.

2. PRZEPISY SZCZEGÓŁOWE PRAWA POLSKIEGO:

- a) Kodeks pracy - uregulowania kodeksu w sprawie przetwarzania danych osobowych pracowników.
- b) Przepisy BHP- dokumentacja powypadkowa, a ochrona danych.
- c) Prawo Autorskie – wizerunek jako dana/informacja, manipulacja wizerunkiem.
- d) Prawo Cywilne – dane osobowe jako dobro.
- e) Kodeks karny - przepisy karne związane z bezpieczeństwem informacji.
- f) Ustawa o świadczeniu usług drogą elektroniczną- adres e-mail jako dana osobowa.

3. PRZEPISY O OCHRONIE DANYCH OSOBOWYCH:

- a) nowelizacja przepisów o ochronie danych osobowych- omówienie podstawowych zmian spójnego Prawa Unijnego dotyczącego Ochrony Danych Osobowych z maja 2018 r.,
 - o wykaz różnic w odniesieniu do aktualnych przepisów,
 - o 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.
 - o Nowe podejście do ochrony danych.

- b) Nowelizacja ustawy o ochronie danych osobowych- **zmiany obowiązujące od 1 stycznia, 26 i 30 maja 2015 r., 1 kwietnia i 19 maja 2016 r.:**
- o „Rejestr Inspektorów Ochrony Danych” - kto może zostać IOD-em, jak zgłosić IOD-a, kto prowadzi rejestr i w jakiej formie,
 - o Zasady tworzenia sprawozdań dla Administratora Danych raportowania incydentów do PUOD,
 - o pozycja Inspektora Ochrony Danych;
 - o jednostki administracji publicznej jako jeden ADO,
 - o dane przedsiębiorców, chronić czy nie chronić - omówienie nowelizacji z dnia 19.05.2016 r.
- c) **Nowe ustawowe obowiązki Inspektora Ochrony Danych w odniesieniu do Administratora Bezpieczeństwa Informacji:**
- o **Kto może, a kto nie może być IOD?**
 - o **Podstawowe zadania IOD,**
 - o **Prowadzenie rejestru czynności przetwarzania w porównaniu z jawnym wykazem zbiorów danych,**
 - o **Plan sprawozdań- zostawić czy zrezygnować,**
 - o **Pouczanie i upominanie osób niestosujących się do Polityki bezpieczeństwa.**
 - o **Jak w praktyce wygląda praca IOD.**
- d) **pojęcie danych osobowych oraz kategorii danych ze szczególnym naciskiem na tzw. „dane wrażliwe” np. stan zdrowia,**
- e) Prezes Urzędu Ochrony Danych- obowiązki i prawa,
- f) szczegółowe omówienie pojęcia Administrator Danych Osobowych,
- g) pozostałe podstawowe pojęcia ustawy o ochronie danych osobowych i RODO,
- h) obowiązki związane z przetwarzaniem danych osobowych:
- o legalne przetwarzanie danych osobowych,
 - o obowiązki informacyjne związane z przetwarzaniem danych osobowych ,
- i) Powierzenie danych osobowych do przetwarzania- **zawieranie umów powierzenia danych osobowych do przetwarzania, przykłady umów powierzenia na nowych zasadach,**
- j) przekazywanie danych osobowych za granice,
- k) przepisy karne ustawy o ochronie danych osobowych.

4. ISO 27001 – podejście Normy do ochrony danych.

5. Panel dyskusyjny.

DZIEŃ II (7h)

1. PROCES ANALIZY RYZYKA I ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIEŃNIA 2004 R. W SPRAWIE DOKUMENTACJI PRZETWARZANIA DANYCH OSOBOWYCH ORAZ WARUNKÓW TECHNICZNYCH I ORGANIZACYJNYCH, JAKIM POWINNY ODPOWIADAĆ URZĄDZENIA I SYSTEMY INFORMATYCZNE SŁUŻĄCE DO PRZETWARZANIA DANYCH OSOBOWYCH:

- a) „Niepotrzebny dokument?”-n szczegółowe omówienie wytycznych co do formy i zawartości dokumentów Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,

- b) osoby odpowiedzialne za opracowanie, wdrożenie i aktualizacje dokumentacji Polityki Bezpieczeństwa,
- c) regulamin korzystania z sieci oraz infrastruktury IT,
- d) wymogi bezpieczeństwa dotyczące pomieszczeń przetwarzania danych osobowych,
- e) zabezpieczenia kryptograficzne przetwarzanych danych osobowych – omówienie narzędzi służących do szyfrowania,
- f) przechowywanie i archiwizowanie danych osobowych,
- g) zagrożenia płynące z sieci Internet - sposoby bezpiecznego korzystania z serwisów www, poczta elektroniczna - zasady bezpiecznej korespondencji,
- h) praktyczne rozwiązania w zakresie opracowania i wdrożenia Polityki Bezpieczeństwa Informacji,
- i) praktyczne rozwiązania w zakresie opracowania i wdrożenia Instrukcji Zarządzania Systemem Informatycznym,
- j) 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:**

- A. Wdrożenie Polityki Bezpieczeństwa oraz powołanie Inspektora Ochrony Danych:
 - **Szacowanie ryzyka,**
 - **Reagowanie na ryzyko,**
 - **Zarządzanie ryzykiem.**
- B. Nadawanie, modyfikacja i odbieranie upoważnienia do przetwarzania danych osobowych (zgodne z RODO).
- C. Zbiory Danych osobowych i czynności przetwarzania:
 - identyfikacja zbiorów i ich elementów,
 - legalizacja elementów zbiorów,
 - identyfikacja zbiorów powierzonych lub otrzymanych w powierzeniu.
- D. Procedury rozpoczęcia i zakończenia pracy z systemem informatycznym.
- E. Legalne źródła danych.
- F. Umowy powierzenia.
- G. Raportowanie incydentów do Prezesa Urzędu Ochrony Danych.
- H. Raport z incydentu i Audyt – z punktu widzenia użytkownika oraz z punktu widzenia IOD.