Orleccy
bezpieczeństwo
i edukacja

Zapraszamy na szkolenie dwudniowe:

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI/INSPEKTOR OCHRONY DANYCH

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

08-09.03.2018 r.

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 wchodzącego w życie w maju 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.**

Orleccy- bezpieczeństwo
i edukacja
Rodzinna 12/3
41-500 CHORZÓW

Tel.: (32) 255 – 55 – 99
Fax: (32) 255 – 55 – 99
E-mail: biuro@orleccy.pl

NIP: 643 164 77 32
REGON: 241728947
www.orleccy.pl

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.:**
   - „Rejestr Administratorów Bezpieczeństwa Informacji" - kto może zostać ABI-m, jak zgłosić ABI-ego, kto prowadzi rejestr i w jakiej formie,
   - Zasady tworzenia sprawozdań dla Administratora Danych i GIODO,
   - Zmiany w rejestracji zbiorów danych - nowe zasady rejestracji i zwolnień z rejestracji zbiorów,
   - pozycja „Nowego" Administratora Bezpieczeństwa Informacji,
   - jednostki administracji publicznej jako jeden ADO,
   - 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:
   - **Kto może, a kto nie może być IOD/ABI?**
   - **Podstawowe zadania IOD/ABI,**
   - **Prowadzenie rejestru czynności przetwarzania w porównaniu z jawnym wykazem zbiorów danych,**
   - **Plan sprawozdań- jak przygotować, co powinien zawierać,**
   - **Pouczanie i upominanie osób niestosujących się do Polityki bezpieczeństwa.**
   - **Jak wygląda praca ABI-ego w Polsce i co się zmieni względem RODO.**

d) pojęcie danych osobowych oraz kategorii danych ze szczególnym naciskiem na tzw. „dane wrażliwe" np. stan zdrowia,

e) Generalny Inspektor Ochrony Danych Osobowych- obowiązki i prawa w odniesieniu do **Urzędu Ochrony Danych,**

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:
   - legalne przetwarzanie danych osobowych,
   - 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 KWIETNIA 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) szczegółowe omówienie wytycznych co do formy i zawartości dokumentów Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym, omówienie poziomów bezpieczeństwa wyszczególnionych w rozporządzeniu **oraz porównanie z RODO,**
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 Administratora Bezpieczeństwa Informacji/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. Sprawozdanie w rozumieniu art. 36. Art. 36a. 2 pkt 1 a Ustawy o ochronie danych osobowych oraz raportowanie incydentów do Urzędu Ochrony Danych.
H. Raport z incydentu i Audyt – z punktu widzenia użytkownika oraz z punktu widzenia ABI.