

Zapraszamy na szkolenie dwudniowe:

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

- najnowsze przepisy,
- szkolenie obejmuje autorskie warsztaty Case Study.

12-13.01.2017 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:

- statystyki wycieków danych,
- konsekwencje wycieków danych,
- przebieg śledztwa po wycieku danych: aresztowanie, przejęcie sprzętu, przesłuchanie,
- konsekwencje zawodowe oraz personalne,
- przykłady handlu danymi w Polsce,
- wartość danych.

2. PRZEPISY SZCZEGÓŁOWE PRAWA POLSKIEGO:

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

3. USTAWA O OCHRONIE DANYCH OSOBOWYCH:

- nowelizacja przepisów o ochronie danych osobowych- omówienie podstawowych zmian spójnego Prawa Unijnego dotyczącego Ochrony Danych Osobowych wchodzącego w życie w maju 2018 r.,**
- 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,

- o Zasady tworzenia sprawozdań dla Administratora Danych i GIODO,
 - o Zmiany w rejestracji zbiorów danych - nowe zasady rejestracji i zwolnień z rejestracji zbiorów,
 - o pozycja „Nowego” Administratora Bezpieczeństwa Informacji,
 - 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 Administratora Bezpieczeństwa Informacji,:**
- o **Prowadzenie jawnego wykazu zbiorów danych (wersja papierowa lub elektroniczna),**
 - o **Plan sprawozdań- jak przygotować, co powinien zawierać,**
 - o **Pouczanie i upominanie osób niestosujących się do Polityki bezpieczeństwa.**
 - o **Jak wygląda praca ABI-ego w Polsce.**
- 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,- porozumienie GIODO z Państwową Inspekcją Pracy,
- f) szczegółowe omówienie pojęcia Administrator Danych Osobowych,
- g) pozostałe podstawowe pojęcia ustawy o ochronie danych osobowych,
- 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,**
- 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. 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,
- b) osoby odpowiedzialne za opracowanie, wdrożenie i aktualizacje dokumentacji Polityki Bezpieczeństwa,
- c) regulamin korzystania z poczty e-mail,
- d) regulamin korzystania z sieci oraz infrastruktury IT,
- e) regulamin korzystania z przenośnych komputerów i urządzeń mobilnych,

- f) wymogi bezpieczeństwa dotyczące pomieszczeń przetwarzania danych osobowych,
- g) zabezpieczenia kryptograficzne przetwarzanych danych osobowych – omówienie narzędzi służących do szyfrowania,
- h) przechowywanie i archiwizowanie danych osobowych,
- i) zagrożenia płynące z sieci Internet - sposoby bezpiecznego korzystania z serwisów www, poczta elektroniczna - zasady bezpiecznej korespondencji,
- j) praktyczne rozwiązania w zakresie opracowania i wdrożenia Polityki Bezpieczeństwa Informacji,
- k) praktyczne rozwiązania w zakresie opracowania i wdrożenia Instrukcji Zarządzania Systemem Informatycznym,
- l) Audyt- zaplanowanie, przeprowadzanie, wdrożenie działań korygujących.

2. ĆWICZENIA.

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. 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
- B. Nadawanie, modyfikacja i odbieranie upoważnienia do przetwarzania danych osobowych
- C. Zbiory Danych osobowych:
 - identyfikacja zbiorów i ich elementów,
 - legalizacja elementów zbiorów,
 - identyfikacja zbiorów powierzonych lub otrzymanych w powierzeniu,
 - rejestracja zbiorów danych.
- 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.
- H. Raport z incydentu i Audyt – z punktu widzenia użytkownika oraz z punktu widzenia ABI.