Temat szkolenia: Ochrona Danych Osobowych

Prowadzący: Paweł Jastrzębski - Informatyk, absolwent studiów podyplomowych w Gnieźnieńskiej Wyższej Szkole Humanistyczno-Menedżerska "Milenium" z zakresu Informatyki i Technologii Komunikacyjnej, od lat zajmujący się problematyką Ochrony Danych Osobowych. Administrator Bezpieczeństwa Informacji, wpisany do ogólnokrajowego Rejestru Administratorów Bezpieczeństwa Informacji prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Członek Rzeczywisty Stowarzyszenia Administratorów Bezpieczeństwa Informacji (SABI). Konsultant, audytor i szkoleniowiec w podmiotach zobowiązanych do stosowania prawa Ochrony Danych Osobowych.

Koszt udziału: 249,00 zł brutto / osoba

Termin: 28 listopada 2017r. (wtorek), godz. 9.00-15.00

Miejsce: Sala szkoleniowa SWPPG – Gostyń, ul. 1 Maja 13/3 (deptak)

PROGRAM SZKOLENIA:

I. Podstawy prawne

1. Konstytucja RP.
2. Ustawa o Ochronie Danych Osobowych.
3. Kodeks Pracy.
4. Ustawa o rachunkowości z 29 września 1994.
5. Ustawa o podatku dochodowym od osób prawnych z dnia 15 lutego 1992 r.
6. Ustawa o podatku od towarów i usług z dnia 11 marca 2004 r.
7. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 roku w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.
8. Odpowiedzialność karna.
9. Rozporządzenia pochodne. Interpretacje i orzecznictwo GIODO – gdzie go szukać?

II. Definicje Danych Osobowych

1. Dane Osobowe.
2. Dane zwykłe i wrażliwe.
3. Definicja zbioru.
4. Formy występowania danych osobowych.
5. Przetwarzanie danych – operacje na danych osobowych.
6. Incydenty.

III. Organizacja ochrony Danych Osobowych w Firmie

1. Podział kompetencji:
   a) Osoby odpowiedzialne.
   b) Kompetencje osób funkcyjnych.
   c) Audyt merytoryczny i techniczny.
   d) Obowiązki wobec GIODO.

2. Wymagania organizacyjne:
   a) Szkolenie pracowników.
   b) Powierzenia danych osobowych (wewnątrz i na zewnątrz organizacji).
   c) Oświadczenia poufności (wewnątrz i na zewnątrz organizacji).
   d) Polityka kluczy.
   e) CV.
   f) Obowiązek informacyjny.
   g) Outsourcing usług (korzyści i zagrożenia).
   h) Rejestr zbiorów Danych Osobowych.
   i) Sprawdzenia.
   j) Kontrole GIODO.
3. Wymagania techniczne.
   a) Wymagania wobec programów komputerowych.
   b) Wymagania wobec systemów serwerowych.
   c) Praca codzienna z komputerem.
   d) Zabezpieczenia (organizacyjne i techniczne).
   e) Kopie zapasowe.
   f) Polityka haseł.

IV. Dokumentacja Ochrony Danych Osobowych

1. Polityka Ochrony Danych Osobowych i dokumenty pochodne.
2. Instrukcja Zarządzania Systemem Informatycznym i dokumenty pochodne.
3. Rejestr Zbiorów Danych Osobowych (Wymaganie GIODO).
4. Sprawdzenia (Wymaganie GIODO).
5. Przykładowe konstrukcje najważniejszych dokumentów:
   a) Ewidencja zbiorów DO.
   b) Polityka kluczy.
   c) Szablon upoważnienia.
   d) Szablon Oświadczenia poufności.
   e) Rejestr Zbiorów Danych Osobowych.
   f) Przykładowe klauzule informacyjne.

V. Zmiany od 2018 roku. Co przynosi RODO? Jak się na te zmiany przygotować?

1. Zakres Ogólnego rozporządzenia o ochronie danych osobowych (RODO).
2. Obowiązki przedsiębiorstw wobec wejścia w życie RODO.
3. Najważniejsze zmiany wprowadzane przez GDPR w stosunku do obecnego stanu prawnego.
4. ABI vs IOD.
   a) kiedy wyznaczenie Inspektora jest obligatoryjne ?
   b) status Inspektora Ochrony Danych
   c) zadania Inspektora Ochrony Danych
   d) odpowiedzialność Inspektora Ochrony Danych
5. Privacy by design.
6. Privacy by default.
7. Obowiązek informacyjny.
8. Uzyskiwanie zgody na przetwarzanie danych.
9. Architektura IT i rozwiązania technologiczne w kontekście RODO
10. Analiza ryzyka.
11. Rejestr przetwarzania.
12. Prawa podmiotów danych na podstawie ogólnego rozporządzenia.
    a) prawo do bycia zapomnianym

b) prawo przenoszenia danych
c) zgoda na przetwarzanie danych osobowych
d) prawo dostępu do danych

VI. Odpowiedzi na pytania i wątpliwości. Dyskusja.