kod szkolenia: HR-MC / MŚP

Bezpieczeństwo informacji i ochrona danych osobowych w MŚP

Dynamiczny rozwój technologii i praca z danymi cyfrowymi sprawiają, że bezpieczeństwo informacji staje się jednym z kluczowych obszarów zarządzania w małych i średnich przedsiębiorstwach. Wyzwania związane z ochroną danych osobowych (RODO), tajemnicą przedsiębiorstwa oraz ryzykami cyberbezpieczeństwa wymagają praktycznej wiedzy, jasnych procedur i świadomego personelu.

Odbiorcy szkolenia

Uczestnicy zdobędą umiejętność projektowania i wdrażania systemu ochrony informacji w swojej firmie, zgodnego z wymogami RODO, innymi wymaganiami prawnymi oraz zasadami bezpieczeństwa organizacyjnego i technicznego.

Adresaci szkolenia

- właściciele i menedżerowie MŚP,
- administratorzy danych, osoby odpowiedzialne za administrację, HR, marketing, jakości, compliance lub IT,
- pracownicy biurowi mający dostęp do danych klientów i partnerów.

Korzyści

Uczestnicy:

- nauczą się oceniać ryzyka i wdrażać adekwatne środki ochrony informacji,
- otrzymają gotowe narzędzia i checklisty (analiza ryzyk, polityka i procedury bezpieczeństwa, rejestr incydentów),
- przygotują własny plan wdrożenia systemu bezpieczeństwa informacji,

- zrozumieją, jak uniknąć kar i błędów wynikających z naruszenia RODO i in. istotnych przepisów,
- uzyskają dostęp do materiałów elektronicznych i konsultacji po szkoleniu.

Program szkolenia

Dzień 1 – Podstawy bezpieczeństwa informacji

- Wprowadzenie i diagnoza potrzeb – cele, kontekst MŚP, główne wyzwania
- Pojęcia i zasady bezpieczeństwa – atrybuty bezpieczeństwa, błędy w MŚP
- Zagrożenia i ryzyka – przegląd głównych zagrożeń bezpieczeństwa informacji
- RODO w pigułce – obowiązki, podstawy przetwarzania, dokumentacja
- System ochrony informacji – systemowe podejście do bezpieczeństwa informacji, standardy i zbiory dobrych praktyk
- Wdrażanie systemu – role, szkolenia, odpowiedzialności, czynniki sukcesu i najczęstsze błędy

Dzień 2 – Warsztat wdrożeniowy

- Powtórka i cele dnia
- Analiza ryzyk w praktyce – warsztat z identyfikacji, analizy i oceny ryzyka
- Projektowanie polityki bezpieczeństwa – tworzenie ram dokumentacji
- RODO i incydenty w praktyce – symulacja obsługi incydentów IT oraz naruszeń ochrony danych (na realnych przykładach)
- Plan wdrożenia i follow-up – tworzenie indywidualnego planu działania i wyznaczanie kamieni milowych.

Oczekiwane przygotowanie uczestnika

Nie są wymagane umiejętności techniczne.

Czas trwania

2 dni / 14 godzin

Język

język – polski
materiały – polski