Basisseminar:

IT-Sicherheitskoordinator/in - IT-Sicherheit meets Datenschutz

Der Grad der Digitalisierung nimmt in allen Branchen immer stärker zu. IT-Sicherheit und Datenschutz werden vom deutschen und auch vom europäischen Gesetzgeber immer stärker gefordert und gefördert. Um diese Anforderungen zu erreichen müssen Unternehmen geeignete technische und organisatorische Maßnahmen treffen, auch im Hinblick zum Schutz vor Cyberkriminalität.

IT-Sicherheit-Koordinatoren beraten und unterstützen die Unternehmensleitung, Kunden, Lieferanten und Partner bezüglich IT-Sicherheit. Sie konzipieren angemessene Sicherheitslösungen entsprechend den geltenden technischen und gesetzlichen Standards und betreuen ihre Realisierung. Außerdem erarbeiten sie mit den Fachkräften der verschiedenen Fachabteilungen und Ebenen gemeinsam Lösungen, beraten bei der Umsetzung und protokollieren die Realisierung. IT-Sicherheit-Koordinatoren werden als Schnittstelle zwischen Unternehmen, den IT-Sicherheitsbeauftragten und den Datenschutzbeauftragten eingesetzt.

Inhalte:

- Rechtliche Grundlagen (BDSG und EU-DSGVO)
- Maßnahmenpaket zur EU-DSGVO
- Grundlagen der IT-Sicherheit
- Aufrechterhalten der IT-Sicherheit
- Erstellen eines IT-Sicherheitskonzepts
- Umsetzen des IT-Sicherheitskonzepts

Termine:

KW 48: 27.11.2018 - 29.11.2018 (max. 15 Personen)
KW 50: 11.12.2018 - 13.12.2018 (max. 15 Personen)

Ort:

Kloster St. Josef
Wildbad 1, 92318 Neumarkt

Preis pro Teilnehmer:

1.100 EUR zzgl. gesetzl. MwSt (EINFÜHRUNGSANGEBOT)

Tag 1

- Rechtliche Grundlagen des Datenschutzes
- Grundlagen Recht
    - IT-Recht und verfassungsrechtliche Grundlagen des Datenschutzes Inhalte/Umsetzung
    - Datenschutzrecht laut EU-DSGVO / BDSG-neu
- Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 DSGVO)
    - Rechtmäßigkeit – Verarbeitung nach Treu und Glauben
    - Transparenz
    - Einwilligung
    - Erforderlichkeiten
- Rechte der betroffenen Person, Datenschutzrechtliches (Art. 15 DSGVO)
    - Recht auf informelle Selbstbestimmung und Rechtsvorschriften des Datenschutzes
    - Zulässige Datenverarbeitungen, Datenverarbeitung für –eigene Zwecke, – fremde Zwecke, internationale Datenübermittlung (innerhalb der EU / außerhalb der EU)

- Auftragsverarbeitung
    - Auswahl des Auftragsverarbeiters
    - Vertragliche Regelung
    - Kontrollrechte
    - Ende des Auftragsverarbeitungsverhältnisses
- Verzeichnis von Verarbeitungstätigkeiten
    - Pflicht zur Erstellung laut Art. 30 EU-DSGVO
    - Form, Inhalt und Vorlage des Verzeichnisses
- Datenschutzbeauftragter
    - Sinn und Pflicht zur Benennung eines DSBs
    - Aufgaben und Schnittstellen
- (IT-)Sicherheit in der Verarbeitung
    - Schutzziele der IT-Sicherheit
        - Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)
        - Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)
        - Verfügbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)
    - IT-Sicherheit ist Chefsache
    - Risikomanagement (Umgang mit Risiken)

Tag 2

- Grundlagen der IT-Sicherheit
    - Informationssicherheit – Datenschutz – IT-Sicherheit
    - Begriffe und Grundkonzepte
    - Aspekte des Sicherheitsmanagements
    - Sicherheitsleitlinie
    - Sicherheitsmaßnahmen
    - Übersicht Angreifer und Angriffsvektoren
- Aufrechterhalten der IT-Sicherheit
    - Integration in den ISMS-Prozess
    - Initiierung des Sicherheitsprozesses
- Aufbau und Struktur eines IT-Sicherheitskonzeptes
    - Begriffsbestimmungen und Überblick
    - Rahmenbedingungen
    - Schutzbedarfsfeststellung

Tag 3

- Umsetzen des IT-Sicherheitskonzepts
    - Akteure
    - Risikobewertung
    - Feststellung des Schutzbedarfes
    - Wichtige IT-Sicherheitsmaßnahmen
- Technische und organisatorische Maßnahmen (TOM)
- Kontrollen durch die Aufsichtsbehörde

- Verletzung des Schutzes personenbezogener Daten
    - Wann liegt eine Verletzung vor?
    - Pflicht zur Meldung an die Aufsichtsbehörde und betroffenen Personen
- Sanktionen und Haftung
- Umgang mit der Aufsichtsbehörde
- Ausarbeitung/Beantwortung rechtlicher Fragestellungen