Inhalte

MODUL RECHT — ONLINETAGE

RECHTSGRUNDLAGEN DER IT-SICHERHEIT UND DES DATENSCHUTZES — 1

Begriffe & Grundlagen des IT-Sicherheitsrechts
Begriffe & Grundlagen des Datenschutzes
Überblick über die wichtigsten Rechtsquellen
Schwerpunkt 1:
Datensicherheit zwischen IT-Sicherheit und Datenschutz
Schwerpunkt 2:
IT-Sicherheit als unternehmerische Sorgfaltspflicht
Schwerpunkt 3:
Grundlagen zur Klausel „Stand der Technik" im IT-Sicherheitsrecht

GRUNDLAGEN DES CORPORATE LAWS UND IT-CORPORATE GOVERNANCE — 1

Begriffe & Grundlagen des Corporate Law
Begriffe & Grundlagen des Corporate Governance
Überblick über die wichtigsten Rechtsquellen
Schwerpunkt 1:
Grundlagen unternehmerischer Sorgfalt (AG, GmbH)
Schwerpunkt 2:
Grundlagen zu Compliance Management Systeme

IT-SICHERHEIT & IT-GOVERNANCE IN DER PRAXIS — 1

IT-Governance – Begriffe & Grundlagen
Frameworks und deren Herkunft
Anwendung der Frameworks
IT Process Management
ITIL Framework
Process Compliance mittels Process Mining

IT-SICHERHEIT UND „VERTRAUEN" ALS BUSINESS-MODEL: CASE-STUDY ZU E-HEALTH — 0,5

Digitale Ökosysteme und digitale Marktplätze (Spannungsfeld: Regulierte und nicht-regulierte Plattformen am Beispiel des ELGA-Projektes)
Umsetzung von Standards und Regulierungen im eHealth Bereich
Regionale und Nationale eHealth-Systeme, rechtliche Herausforderungen und Umsetzungsstrategien

ARBEITGEBER/INNEN, DATENSCHUTZ & IT-SICHERHEIT — 0,5

BYOD
IT-Sicherheit und Überwachung der Arbeitnehmer/innen
Private E-Mailnutzung
Private Nutzung der Firmen-IT-Infrastruktur (E-Mail, WLAN, etc.)

MODUL RECHT — ONLINETAGE

CYBERCRIME UND IOT-STRAFRECHT — 0,5

Phänomenologie Cybercrime und IoT-Strafrecht
Präventionsstrategien gegen Cybercrime
Strategien zur Aufarbeitung von Cybercrime-Vorfällen
Die Haftung des Unternehmensvorstandes für Cybersicherheit aus versicherungsrechtlicher Perspektive

IT-SICHERHEITSREICHT, RISIKOMANAGEMENT & CYBERVERSICHERUNGSRECHT — 0,5

Case Studies zu den gesetzlichen Anforderungen laut NIS-RL und Aufbau eines Policy-Frameworks unter Berücksichtigung von Anforderungen aktueller Cyberversicherungen
Case Studies zur gesetzlichen Generalklausel „Stand der Technik" am Beispiel von Information Risikomanagement
Frameworks zur Ermittlung der aktuellen Cyberbedrohung in Euro
Case Studies zur Technologiestack Bewertung nach dem NIST Cybersecurity Architecture Framework

MODUL TECHNIK — ONLINETAGE

TECHNISCHE GRUNDLAGEN ZUR IT-SICHERHEIT FÜR NICHT-INFORMATIKER/INNEN — 2,5

Grundbegriffe, Schutzziele & Dimensionen der IT-Sicherheit
Einführung in die symmetrische und asymmetrische Kryptographie, inkl. E-Mail-Sicherheit und digitale Signaturen
Einführung in die praktische IT-Sicherheit, inkl. gängiger Begriffe und Gegenmaßnahmen
Einführung in den technischen Datenschutz

IMPLEMENTATIONSSTRATEGIEN — 2,5

Überblick über die relevanten Standards im Gebiet der Informationssicherheit
Einführung in Information Security Management Systeme (ISMS)
Planung und Implementierung eines ISMS im Unternehmen

9 MODULE | 10 ONLINETAGE* | 10 ECTS

*exkl. Vor- und Nachbereitungen, Selbststudium, Reflexionspapiere, Projektarbeiten, Abschlussarbeit, u.ä.