

Rechtliche Aspekte der Digitalen Transformation (W3M11308)

Legal aspects of digital transformation

FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
W3M11308	-	1	Prof. Dr. Sebastian Richter	Deutsch/Englisch

EINGESETZTE LEHRFORMEN

LEHRFORMEN	LEHRMETHODEN
Vorlesung, Übung	Lehrvortrag, Diskussion, Gruppenarbeit

EINGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Klausur	120	ja

WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
135	42	93	5

QUALIFIKATIONSZIELE UND KOMPETENZEN

FACHKOMPETENZ

Die Studierenden verfügen über vertieftes Wissen über gesellschaftliche, rechtspolitische und IT-rechtliche Rahmenbedingungen für den Wirtschaftsstandort Deutschland, Europa und global im Kontext der Digitalisierung. Die Studierenden können Lösungsstrategien der digitalen Transformation hinsichtlich rechtlicher Aspekte grundsätzlich einordnen und in der Interaktion mit Fachspezialist*innen beurteilen.

METHODENKOMPETENZ

Studierende sind befähigt, selbstständig sowohl mit bekannten als auch unbekanntem bzw. sich neu entwickelnden gesetzlichen Vorschriften im IT-Recht umzugehen und diese zielgerichtet für die Transformation anzuwenden.

Die Studierenden verstehen die Systematisierung relevanter IT-Rechtsvorschriften und können auf dessen Grundlage in Zusammenarbeit mit Rechtsspezialist*innen die Compliance von Unternehmen in Digitalisierungsfragen sicherstellen.

PERSONALE UND SOZIALE KOMPETENZ

-

ÜBERGREIFENDE HANDLUNGSKOMPETENZ

Die Studierenden sind in der Lage, technisch-organisatorische sowie betriebswirtschaftliche Prozesse im unternehmerischen Kontext unter digitalrechtlichen Gesichtspunkten einzuordnen, zu bewerten und compliance-konform zu planen und umzusetzen.

LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Rechtliche Aspekte der Digitalen Transformation	42	93

Verfassungsrechtliche und ethische Grundpfeiler von Datenschutz und Cybersicherheit als Grundlagen von digitaler Transformation
Funktionsweise des Rechtsetzungsprozesses in der EU und in Deutschland
Rechtspolitische Diskussionen und Erwägungen für die aktuelle Rechtsetzung zu Datenschutz und Cybersicherheit
Systematischer Überblick über aktuelle EU-Gesetze sowie nationale Rechtsvorschriften zu Datenschutz und Cybersicherheit
Rechtsrahmen I (allgemeiner Datenschutz): Prinzipien und Erlaubnistatbestände einer Datenverarbeitung gem. EU DS-GVO, BDSG-neu inkl. diskussionswürdiger Problemstellungen, zB Reichweite und Praktikabilität von Einwilligungserklärungen in die Verarbeitung personenbezogener Daten, Entwicklung alternativer Instrumente
Rechtsrahmen II (bereichsspezifischer Datenschutz): Spezifische Erlaubnistatbestände zur Datenverarbeitung für Zwecke der Cybersicherheit (zB EU NIS-RL, EU Cybersecurity Act, IT-SiG und IT-SiG 2.0)
Rechtsrahmen III (Sonderprobleme/spezielle Fragestellungen): ZB ePrivacy, Drittstaatenübermittlung (zB „Privacy Shield“), staatliche Nutzung von zero-day-exploits, Einsatz von staatlicher Malware zur Durchführung von Online-Durchsuchungen/Quellen-TKÜ (ZITIS), Informationsverarbeitung zur Abwehr und Verfolgung von Cyberstraftaten, Key-Escrowing, Videoüberwachung, Einbindung von Privatunternehmen in die Erfüllung hoheitlicher Aufgaben, Zentralisierung von Behördenkompetenzen, Risiken durch Informationsvernetzung
Rechtsrahmen IV (internationale Regulierung von Datenschutz und Cybersicherheit): Rechtsvergleichende Zusammenschau und Diskussion über internationale bereichsspezifische Regulierungsansätze, so beispielsweise in China, USA, Russland, Israel; zunehmende Bedeutung internationaler Rechtsetzung für die europäische/deutsche Wirtschaft, mit der Rechtsetzung verbundene gesellschaftspolitische Problem- und Fragestellungen in den jeweiligen Ländern, die mit der digitalen Transformation einhergehen

BESONDERHEITEN

-

VORAUSSETZUNGEN

-

LITERATUR

Es wird jeweils die aktuellste Auflage zu Grunde gelegt.

Kipker, D.-K.: Cybersecurity: Rechtshandbuch, München.
Kühling, J.; Buchner, B.: DS-GVO – BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar, München.
Terhaag, M.: IT-Sicherheitsgesetz. Auswirkungen, Entwicklung und Materialien für die Praxis, Köln.
Hoffmann, M.; Kitz V.; Leible, S.: IT-Compliance. IT und öffentliche Sicherheit, o.O.
Harich, T. W.: IT-Sicherheitsmanagement: Arbeitsplatz IT Security Manager, Heidelberg u.a.
Eckert, C.: IT-Sicherheit. Konzepte – Verfahren – Protokolle, Berlin, Boston.
Hauschka, C. E.; Moosmayer, K.; Lösler, T.: Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen, München.
Simitis, S.: Bundesdatenschutzgesetz. NomosKommentar, Baden-Baden