Grundlagen Datenschutz, IT-Sicherheit und IT-Recht (SMDiSA_07)

Basics – Data Protection, IT Safety and IT Law

FORMALE ANGABEN ZUM MODUL

MODULNUMMER	VERORTUNG IM STUDIENVERLAUF	MODULDAUER (SEMESTER)	MODULVERANTWORTUNG	SPRACHE
SMDiSA_07	-	1	Prof. Dr. Tobias Straub	Deutsch

EINGESETZTE LEHRFORMEN

LEHRFORMEN	LEHRMETHODEN
Vorlesung	Lehrvortrag, Diskussion, Fallstudien

EINGESETZTE PRÜFUNGSFORMEN

PRÜFUNGSLEISTUNG	PRÜFUNGSUMFANG (IN MINUTEN)	BENOTUNG
Mündliche Prüfung kombiniert mit Seminararbeit	Siehe Pruefungsordnung	ja

WORKLOAD UND ECTS-LEISTUNGSPUNKTE

WORKLOAD INSGESAMT (IN H)	DAVON PRÄSENZZEIT (IN H)	DAVON SELBSTSTUDIUM (IN H)	ECTS-LEISTUNGSPUNKTE
150	40	110	5

QUALIFIKATIONSZIELE UND KOMPETENZEN

HANDLUNGSKOMPETENZ

- Die Studierenden können die fachlichen Anforderungen ihrer Einrichtung an IT-Systeme und -Prozesse aufnehmen und systematisch daraufhin untersuchen, ob sie mit rechtlichen und sicherheitstechnischen Rahmenbedingungen vereinbar sind.
- Die Studierenden wissen Bescheid über die zentralen Methoden und Techniken der IT-Sicherheit und des Datenschutzes und können Problemstellungen durch deren Einsatz zielgerichtet und effizient lösen.
- Die Studierenden kennen die für den betrieblichen Kontext maßgeblichen Rechtsgrundlagen und sind in der Lage, beim Einsatz von IT-Systemen oder der Durchführung von IT-Projekten rechtliche Risiken und Gestaltungsmöglichkeiten frühzeitig erkennen zu können. Dadurch helfen sie, Haftungsrisiken für ihre Einrichtung zu vermeiden.

SELBSTKOMPETENZ

- Die Studierenden sind in der Lage, sich bei der Planung und Evaluation von IT-Systemen und Prozessen mit den Spezialisten aus den jeweiligen Bereichen (z. B. Justitiariat, Datenschutz-/Informationssicherheitsbeauftragte) auszutauschen und die Anforderungen ihrer Einrichtung der Sozialen Arbeit adäquat zu kommunizieren.

SOZIAL-ETHISCHE KOMPETENZ

- Die Studierenden sind dafür sensibilisiert, dass eine Verarbeitung personenbezogener Daten in das informationelle Selbstbestimmungsrecht von Mitarbeiterinnen und Mitarbeitern sowie Klientinnen und Klienten eingreift.
- Die Studierenden sind sich bewusst, dass IT-Sicherheit und Datenschutz zuweilen in einem Spannungsverhältnis stehen, und sie sind in der Lage, einen Ausgleich zu finden.
- Die Studierenden können die getroffenen Maßnahmen und Festlegungen kritisch reflektieren, um diese nötigenfalls dem technischen Fortschritt oder geänderten rechtlichen Rahmenbedingungen anzupassen.

WISSENSKOMPETENZ

- Die Studierenden kennen die relevanten rechtlichen Rahmenbedingungen des Einsatzes von IT-Systemen.
- Die Studierenden haben ein Grundverständnis für die Herausforderungen, Ziele und Methoden der IT-Sicherheit und des Datenschutzes entwickelt.
- Die Studierenden können proaktiv die in Einrichtungen der Sozialen Arbeit auftretenden typischen Fragestellungen mit Bezug zu Datenschutz, IT-Sicherheit oder IT-Recht identifizieren und hierfür Lösungsansätze entwickeln. Dabei sind sie in der Lage, die in der Vorlesung vermittelten Vorgehensweisen auf konkrete ethische, rechtliche oder technische Fragestellungen in der Praxis anzuwenden.
- Sie können rechtliche Vorgaben, insbesondere aus dem Datenschutzrecht, sowie technische Schutzmaßnahmen frühzeitig bei der Planung, Auswahl und Einführung von IT-Systemen berücksichtigen.

LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM
Grundlagen Datenschutz, IT-Sicherheit und IT-Recht	40	110

LERNEINHEITEN UND INHALTE

LEHR- UND LERNEINHEITEN	PRÄSENZZEIT	SELBSTSTUDIUM

Grundlagen IT-Recht (Auswahl aus den folgenden Themen):
- Arten von IT-Verträgen für Software, Hardware, Dienstleistungen (Kauf-, Werk-, Dienstvertrag)
- Vertragsgestaltung bei IT-Projekten (Beauftragung von Dritten, Outsourcing)
- Software-Lizenzverträge, Lizenzierungsmodelle, Open Source
- Haftung/Gewährleistung
- Gestaltung von Nutzungsbedingungen, Benutzungsordnungen, Betriebsvereinbarungen zur Nutzung von IT-Systemen
- rechtliche Anforderungen für die Dokumentation
- Signaturgesetz
- Intellectual Property, Urheberrecht
- Kopierschutzsysteme
- Geheimhaltungserklärungen
- TKG/TMG (Provider-Haftung, Impressumspflicht)
- Computer-Strafrecht (File Sharing, Hacking, § 202c)
- Zugriffsmöglichkeiten der Strafverfolgungsbehörden

Grundlagen des Datenschutzes:
- informationelles Selbstbestimmungsrecht, Rechtsgrundlagen und grundlegende Prinzipien
- Anforderungen an Einwilligungen, Datenverarbeitung im Auftrag, gemeinsame Verantwortlichkeit, Datenschutz im Arbeitsrecht
- technisch-organisatorische Maßnahmen, Rechenschafts- und Dokumentationspflichten

Grundlagen der IT-Sicherheit:
- Beispiele aktueller Bedrohungen, typische Angriffsvektoren
- grundlegende Begriffe und Konzepte der IT-Sicherheit
- gängige Mechanismen für die Umsetzung von Schutzzielen und ausgewählte Maßnahmen (z. B. Biometrie, Verschlüsselung)
- Faktor Mensch (Social Engineering, Security Awareness)
- Standards in der IT-Sicherheit
- Vorgehensmodelle zum Informationssicherheitsmanagement

BESONDERHEITEN

Kombinierte Prüfungsleistung: mündliche Prüfung und Seminararbeit

VORAUSSETZUNGEN

Zusätzliche Voraussetzung für die Belegung im Rahmen eines Masterstudiums: Bachelorabschluss mit 180 ECTS
Alle im Rahmen des Zulassungsprozesses durch die jeweilige Wissenschaftliche Leitung festgelegten Grundlagenmodule sind erfolgreich abgeschlossen.

LITERATUR

Es wird jeweils die aktuellste Auflage zu Grunde gelegt.
IT-Recht und Datenschutz:
- Astrid Auer-Reinsdorff (Hrsg.) Handbuch IT- und Datenschutzrecht, C.H. Beck
- Eugen Ehmann: Lexikon für das IT-Recht 2019: Die 150 wichtigsten Praxisthemen
- Meinhard Erben: Allgemeine Geschäftsbedingungen von IT-Verträgen, Springer Gabler
- Meinhard Erben: Gestaltung und Management von IT-Verträgen, Springer Gabler
- Marion Hundt: Datenschutz in der Kinder- und Jugendhilfe: Praxishandbuch für die sozialpädagogische Arbeit, Walhalla und Praetoria
- Karl Wolfhart Nitsch: Informatikrecht: Grundlagen, Rechtsprechung und Fallbeispiele, Springer Gabler
- Mark Rüdlin, Dirk Otto: Datenschutz in sozialen Einrichtungen, Mediengruppe Oberfranken
- Rolf Schwartmann (Hrsg.): Praxishandbuch Medien-, IT- und Urheberrecht, C.F. Müller
- Fachdatenbanken (Juris, Beck Online) und Kommentar-Literatur

IT-Sicherheit:
- Michael Brenner et al.: Praxisbuch ISO/IEC 27001, Hanser
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, Oldenbourg
- Thomas Harich: IT-Sicherheitsmanagement: Praxiswissen für IT Security Manager, mitp
- Heinrich Kersten et al.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, Springer Verlag
- Tobias Schrödel: Hacking für Manager, Gabler