

| | | | | | |
|--|---|---|---------------------|-------------------------------|------------|
| Modul INF-BSc-323: Grundlagen der Data Privacy (GDP) | | | | | |
| identisch mit: INF-BL-323: Grundlagen der Data Privacy (Informatik Lehramt Bachelor) INF-ML-323: Grundlagen der Data Privacy (Informatik Lehramt Master) | | | | | |
| Englischer Modultitel: Foundations of Data Privacy | | | | | |
| Studiengänge: Bachelorstudiengang Informatik , Bachelorstudiengang Angewandte Informatik | | | | | |
| Turnus nach Ankündigung | Dauer 1 Semester | Studienabschnitt ab 5. Semester | Credits 4 | Aufwand 120 (45/75) | |
| 1 | Modulstruktur | | | | |
| | Nr. | Element / Lehrveranstaltung | Typ | Credits | SWS |
| | 1 | Grundlagen der Data Privacy | V | 2 | 2 |
| | 2 | Übungen zu Grundlagen der Data Privacy | Ü | 2 | 1 |
| 2 | Lehrveranstaltungssprache: Deutsch und Englisch (Insbesondere soll der zweite Teil im Rahmen des International Summer Programs angeboten und daher auf Englisch gehalten werden.) | | | | |
| 3 | <p>Lehrinhalte</p> <p>Datenverarbeitungssysteme müssen bei der Verarbeitung, Speicherung und Übermittlung personenbezogener Datenschutz berücksichtigen. In diesem Kurs werden die grundlegenden Algorithmen von privatsphäreschützenden Systemen vermittelt</p> <ol style="list-style-type: none"> 1. Einführung in den Datenschutz (Risiken der Re-Identifizierung, Ebenen und Begriff des Datenschutzes, Taxonomie der Datenschutzdefinitionen) 2. Datenschutz durch Aggregation (Datenaggregationsmethoden, Datennutzen bei Aggregation, Kennzeichnungsproportionen) 3. Datenschutz durch Secret Sharing (Sichere Mehrparteien-Berechnungen) 4. Privatsphäre durch Sketches (Streaming Algorithmen, verlustbehaftete Zählung, Reservoir Sampling, Count-Min Sketches, Flajolet-Martin Sketches) 5. Vertraulichkeit durch Datenperturbation (Filterung, Vereinfachung, Verallgemeinerung, Hashing) 6. Privatsphäre durch differentielle Privatsphäre (Konzept der Differential Privacy, Laplacian Noise, datenschutzgerechte Datenveröffentlichung) 7. Grundlagen der Kryptographie (Diskreter Logarithmus, Diskrete Wurzeln, Erweiterter Euklidischer Algorithmus, Chinese Remainder Theorem) 8. Privatsphäre durch Kryptographie (Symmetrische vs. asymmetrische Kryptographie, RSA) 9. Privatsphäre durch homomorphe Verschlüsselung (Pailliers homomorphes Verschlüsselungsverfahren, Shamir's Secret Sharing, E-Voting-Systeme) 10. Datenschutzbestimmungen (GDPR, UNDG) 11. Ethik und Big Data (Bewertung von Datenschutz und Ethik, Sensibilisierung für ethische Herausforderungen durch Big Data) <p>Die Hauptziele des Kurses sind:</p> <ul style="list-style-type: none"> • Lernen der Herausforderungen des Datenschutzes, • Vermittlung von Kenntnissen von privacy-preserving Methoden für die Speicherung/Übertragung/Analyse von Daten und deren Veröffentlichung, • Erlernen von Privacy-by-design Analysemethoden, • Einführung zu gesetzlichen Regelungen in Bezug auf Datenysteme, <p>Vorstellung des ethischen Beurteilungsprozesses.</p> <p><i>Content</i></p> <p>Data processing systems must take into account the privacy of individuals when processing, storing and transmitting personal data. This course teaches the basic algorithms of privacy-protecting systems.</p> | | | | |
| 4 | <p>Kompetenzen</p> <p>Nach Abschluss des Kurses sollen die Teilnehmer*innen in der Lage sein:</p> <ul style="list-style-type: none"> • die vielfältigen Herausforderungen des Datenschutzes bei der Speicherung, Verarbeitung und Modellierung von Big Data, Datenströmen oder episodischen Daten zu erklären und zu interpretieren • Differential Privacy zu verwenden, | | | | |

| | | |
|---|---|--|
| | <ul style="list-style-type: none"> • Methoden des Secret Sharing zu verwenden, • Kryptographische Prinzipien darstellen, • eine Ethikbewertung eines Softwaresystems durchführen. | |
| 5 | Prüfungen <i>Modulprüfung:</i> Klausur oder mündliche Prüfung ^{BOSS-Nr. 88894} <i>Studienleistung:</i> <ul style="list-style-type: none"> • aktive Mitarbeit in der Übung und Erreichen der Mindestpunktzahl bei den Übungsaufgaben ^{BOSS-Nr. 8844} Die Studienleistung ist Voraussetzung für die Teilnahme an der Modulprüfung | |
| 6 | Prüfungsformen und -leistungen <input checked="" type="checkbox"/> Modulprüfung <input type="checkbox"/> Teilleistungen | |
| 7 | Teilnahmevoraussetzungen <i>Erfolgreich abgeschlossen:</i> -keine- <i>Wünschenswerte Kenntnisse:</i> Grundlegende Kenntnisse der Mathematik (insbes. Ringe), und Grundlagen der Datenwissenschaft | |
| 8 | Modultyp und Verwendbarkeit des Moduls Wahlmodul in den Bachelor-Studiengängen Informatik und Angewandte Informatik | |
| 9 | Modulbeauftragte/r Prof. Dr. Th. Liebig | Zuständige Fakultät Informatik |
| | | <small>Beschluss Fakultätsrat 17.08.2022</small> |