Reg No: DVAD30/20181

Faculty of Health, Science and Technology
Computer Science

Syllabus

Privacy by Design

Course Code:	DVAD30
Course Title:	Privacy by Design *Inbyggd integritet*
Credits:	7.5
Degree Level:	Master's level
Progressive Specialisation:	Second cycle, has only first-cycle course/s as entry requirements (A1N)

Major Field of Study:

DVA (Computer Science)

Course Approval

The syllabus was approved by the Faculty of Health, Science and Technology 2017-09-13, and is valid from the Spring semester 2018 at Karlstad University.

Prerequisites

Upper secondary level English 6 or B. Computer Science 30 ECTS cr, or three years of work experience in the IT sector, or equivalent

Learning Outcomes

Upon completion of the course, students should be able to:
- give an account of basic legal privacy concepts, regulations and principles, and of major court decisions at national and European level,
- analyse privacy challenges and the risks of ICT and applications,
- map legal privacy principles to technical privacy concepts,
- give an account of the basic security and privacy enhancing technologies,
- relate security and privacy goals to mechanisms and technologies,
- explain when and how to apply different privacy enhancing technologies.
- give an account of the concepts of privacy, data protection, privacy enhancing technologies, privacy by design, and privacy impact assessment,
- relate privacy by design to personal privacy, data protection, privacy enhancing technologies and basic human rights,
- explain how privacy by design and privacy impact assessment are used in regard to privacy enhancing technologies,
- demonstrate broad knowledge of alternative approaches to managing information privacy and data protection in organizations,
- demonstrate deepened insight into one method for managing information privacy,
- demonstrate analytical skills in risk and effect analysis of privacy protection,
- demonstrate broad knowledge of privacy control selection methods, and deepened insight into the concept of privacy controls,
- explain the fundamental principles of architectural tactics for privacy and privacy patterns,

- list relevant privacy patterns,
- analyse the usage/occurrence of privacy patterns in a given system context,
- apply appropriate architectural tactics for privacy and privacy patterns in a given systems context and for a given set of privacy requirements.

Content

The course comprises five modules.

Module 1 Introduction to Privacy and the GDPR

The module includes the definitions, history and foundations of privacy with an emphasis on the challenges in information and communication technology. The focus is on the European and national (Swedish) laws regulating privacy, data protection and cyber safety, including agreements on transferring personal information beyond the EU. Some important decisions of the EU court in this area are discussed.

Module 2 Privacy Enhancing Technologies

The module introduces security and privacy mechanisms and technologies and proceeds to focus on how security and privacy mechanisms can be used to solve practical and theoretical problems, along with discussions of their advantages and disadvantages.

Module 3 Designing for Privacy

The module introduces the foundations of privacy, data protection, and privacy enhancing technologies, and focuses on the concepts of privacy by design and privacy impact assessments by exploring the relevant background, their relationship to the foundation and fundamental human rights, and by introducing relevant methods.

Module 4 Privacy Management

The module deals with privacy management as part of an organization's information security management. It introduces approaches to privacy management, provides deepened insight into one management approach, and explains how privacy threats can be anticipated and mitigated. Privacy risk and impact analysis are included in the management cycle, as is the selection of privacy control mechanisms.

Module 5 Privacy Patterns for Software Design

The module deals with privacy aspects during software design. It particularly focuses on architectural tactics and patterns as reusable conceptual solutions to recurring privacy problems. It also outlines how to use these concepts in agile development settings in order to engineer privacy into software.

The following components are included:
- Fundamental concepts of architectural tactics and patterns
- Privacy as quality attribute of software systems
- Introduction to privacy patterns, privacy anti-patterns, and privacy dark patterns
- Applying privacy patterns in agile development.

Reading List

See separate document.

Examination

Assessment is based on a written exam and hand-in assignments.

Grades

One of the grades Distinction (VG), Pass (G), or Fail (U) is awarded in the examination of the course. Engineering students are awarded one of the grades Pass with Distinction (5), Pass with Some Distinction (4), Pass (3) or Fail (U).

Quality Assurance

Follow-up relating to learning conditions and goal-fulfilment takes place both during and upon completion of the course in order to ensure continuous improvement. Course evaluation is partly based on student views and experiences obtained in accordance with current regulations and partly on other data and documentation. Students will be informed of the result of the evaluation and of any measures to be taken.

Course Certificate

A course certificate will be provided upon request.

Additional information

The courses DVAD31, DVAD32, DVAD33, DVAD34 and DVAD35 cannot be included in the same degree programme as DVAD30.

The local regulations for studies at the Bachelor and Master levels at Karlstad University stipulate the obligations and rights of students and staff.