

|  |
| --- |
|  |

Faculty of Health, Science and Technology

Computer Science

**Syllabus**

**Privacy by Design   
– Data Protection: Concepts, Technology, Implementation and Management**

## **Course Code:** 7DAV021

## **Course Title:** Privacy by Design – Data Protection: Concepts, Technology, Implementation and Management

## *Inbyggd integritet – Dataskydd: Begrepp, teknologi, tillämpning och verksamhetsstyrning*

## **Credits:** 5 ECTS

**Degree Level:** Doctoral

## **Course Approval**

The syllabus was approved by the Faculty of Health, Science and Technology,   
19 June 2019 and is valid from the autumn semester 2019.

## **Language of instruction**

The instruction language is English.

## **Prerequisites**

## Participants must be enrolled in a PhD program. The course requires basic-level understanding of computing, data processing and algorithms.

## **Learning Outcomes**

This course implements the following researcher education learning goals defined by the Swedish higher education regulation:

* (G1) Knowledge and understanding in the research area
* (G2) Contemporary specialist knowledge in a specific area of the discipline
* (G3) Show ability to critically, independently and creatively and with scientific precision identify and formulate questions
* (G4) Show ability for research-ethical judgement in own research
* (G5) Show insight into sciences potential and limitations, its role in society and human responsibility in how research is being used
* (G6) Show ability to identify own need for more knowledge and to show responsibility for own knowledge development.

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 (G1, G2, G5),
* analyse privacy challenges and the risks of ICT and applications (G3, G4, G6),
* map legal privacy principles to technical privacy concepts (G2),
* give an account of the basic security and privacy enhancing technologies (G1),
* relate security and privacy goals to mechanisms and technologies (G2),
* explain when and how to apply different privacy enhancing technologies (G2, G4, G5).
* give an account of the concepts of privacy, data protection, privacy enhancing technologies, privacy by design, and privacy impact assessment (G1, G2),
* relate privacy by design to privacy, data protection, privacy enhancing technologies, and fundamental human rights (G4,G5, G6),
* explain how privacy by design and privacy impact assessments are used (G2).
* demonstrate broad knowledge of alternative approaches to managing information privacy and data protection in organizations (G1),
* demonstrate deepened insight into one method for managing information privacy (G2),
* demonstrate analytical skills in risk and effect analysis of privacy protection (G2,G3),
* demonstrate broad knowledge of privacy control selection methods, and deepened insight into the concept of privacy controls (G1, G2).
* explain the fundamental principles of architectural tactics for privacy and privacy patterns (G1),
* list relevant privacy patterns (G2),
* analyse the usage/occurrence of privacy patterns in a given system context (G2,G3,G6),
* apply appropriate architectural tactics for privacy and privacy patterns in a given systems context and for a given set of privacy requirements (G2).

## **Course Content**

The course comprises five modules. The course content will be provided on an e-learning platform in self-study format. Registration and enrolment synchronized with the reading cycle are necessary for examination.

## 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 assessment by mandatory quiz in each module, a written exam and hand-in assignments in each of the course modules.

## **Grades**

One of the grades Fail (U) or Pass (G) will be awarded after examination.

## **Quality Assurance**

## The course convenor has a duty to encourage a continuous dialogue on learning processes and goal fulfilment. A written evaluation is carried out at the conclusion of the course combined with a joint student-teacher discussion of all aspects commented on. The result of the evaluation is collated and made available in accordance with *The Higher Education* Ordinance, Chapter 1, § 14.

## **Course Certificate**

## Course certificate is issued on request.