

# Secure Software Engineering Lab

## Lab 5: Privacy Engineering

Institute of Software Security (E-22)

### 1. Objectives

Apply the knowledge acquired in the lectures on the following areas of software security:

- Identification of privacy threats.
- Elicitation of privacy requirements.
- Selection of privacy tactics and Privacy-Enhancing Technologies (PETs).

### 2. Tasks

#### 1. Create a Data Flow Diagram (DFD) of the Metaverse.

- Use the case study description as a starting point plus the supplementary material.
- Focus on (i) login, (ii) registration, and (ii) befriending processes.
- You can re-use the DFDs from Lab 3.

#### 2. Elicit privacy threats.

- Map DFD elements to LINDDUN threat categories.
- Elicit privacy threats using LINDDUN threat trees catalog.
- Document the elicited threats using LINDDUN documentation template.

#### 3. Manage privacy threats.

- Prioritize the privacy threats according to their risk ( $risk = impact \times likelihood$ ).
- Map threats to mitigation strategies (use LNDDUN template).
- Refine mitigation strategies and select suitable PETs.

#### 4. Conduct a Privacy Impact Assessment (PIA) using the CNIL tool.

- Consider the processing of personal data from Virtual Reality (VR) headsets.

### 3. Materials

Case study, lecture slides, lab slides, LINDDUN documentation templates and threat catalog.