

Exercise 1

- Pick an arbitrary complex dataset (e.g. smart home data, medical records, ...)
 1. What information can you infer from the dataset on each individual?
 2. What other databases could you link the dataset to?
 3. What other actors might have which interests towards that dataset?
 4. How can the dataset be anonymized/pseudonymized?
 5. By whom?
 6. What exact information leakage would be stopped this way?
 7. What about „Artificial Intelligence“? Could it overcome your approach? How?
- Is full anonymization still feasible today?

Exercise 2

- Pick an arbitrary data processing scenario (e.g. online shop, car navigation system, ...)
 1. Write down all personal data processed/stored
 2. Write down all metadata surfacing
 3. Write down all stakeholders involved in your scenario
 4. Iterate over the six protection goals:
 - a. Is there any relevance of the protection goal towards your scenario?
 - b. If so, towards which data, and by which stakeholder?
 - c. What is the risk imminent to said protection goal?
 - d. How could the fulfillment of said protection goal be enhanced?