Patterns, policies, and argumentations for creating privacy-aware high-tech products

Privacy and security are essential for modern high-tech systems, such as cars, trains, and medical devices. These requirements shall be addressed in system architectures without compromising safety. A systematic approach to consider them include identifying relevant stakeholders, system parameters, aspects, and building blocks. Tracing and tracking links between them and agreements between owners of solution elements are important for highlighting how decisions taken in one part impact others.

For example, think of tracking driver’s health data, so the car can safely stop in case of emergency.

- How to handle data if a car tracks your health using its own sensors? If you as a driver have wearable sensors? If those are linked to your phone? To your car? To a gateway in your house?
- Who owns the sensor data? If multiple systems interact and merge data, who is in control of the data? What are relevant patterns and policies? How to think of GDPR in such a case?
- How to build an argument for system developers (in context of product security) that one solution is better than another? What if there are severe limitations for solutions?

In this MSc project you will work with ESI (www.esi.nl), a TNO joint innovation center, who leads reference architecture efforts in a large EU project SECREDAS, which consists of 69 partners. You will familiarize yourself with Model-Based System Architecting methodology and the supportive tool. You will use those to structure and analyze your results. Your research and feedback will provide inputs for future development of practical approaches and solutions.

For more information please contact:
- Nicola Zannone (N.Zannone@tue.nl);
- Alexandr Vasenev (Alexandr.Vasenev@tno.nl).