1 PRIVACY GUIDELINES

Sensors, mobile phones, wearable objects, Rfid tags, cameras, middleware components, have a common feature: they are all points of entrance of data, which can include personal data. As the players of the IoT landscape heavily leverage on personal data to deliver services and increase consumers' welfare, personal data protection and security are key elements in the "value creation chain" of IoT.
U4IoT has therefore elaborated a set of Privacy and Data Protection Guidelines for the LSPs, whereby the main actions, methodologies and safeguards for personal data protection are identified, in order to enable the LSPs to reap the potential of IoT technologies while protecting users' rights.

2 PRIVACY GAME

2.1 Serious game about privacy – general goals

The serious game about privacy is part of U4IoT CSA project. It intends to support end-user engagement in the five Large Scale Pilots (LSPs) on the Internet of Things (IoT) financed by the European Commission and other partners, such as the Swiss Ministry for Research and Education.

One objective of U4IoT is to ensure that end-user rights, related to data protection, are fully respected. Beyond the reputational risks, the newly adopted General Data Protection Regulation (GDPR) imposes strict rules and obligations, with legal and financial risks for those who would not respect them.

In this context, Archimede Solutions (AS) is in charge of developing a serious game to raise awareness about the privacy aspects connected to IoT in the LSPs, offering an easier way to understand complicated legal and IoT-related concepts.

2.2 Objectives of the serious game

The aim of the serious game on privacy and GDPR for the LSPs developed in U4IoT is:

- To educate the LSPs stakeholders to the key principles of data protection, as stated in the General Data Protection Regulation, and other complementary obligations (such as the Swiss Act on Data Protection for pilots located in Switzerland);
- To raise awareness on the main risks related to data protection with IoT deployments;
- To serve as a useful tool for the LSPs;
- To translate complex legal norms into clear and easily understandable principles.
- To reduce the risks of non-compliance with the Data Protection Obligation in the five LSPs.
- To demonstrate successful adoption and use by a large number of players in the five LSPs.

Finally, the task will:

- Evaluate and demonstrate the achievement of the above mentioned objectives;
- Extract learnt experiences to improve and guide the development of future serious games on privacy.

2.3 Target groups of users

The aim intends to serve and address the following groups of users, in decreasing priority:

- 1. LSP consortia: the members of the consortia in charge of implementing and deploying the LSPs are the first priority group. They should learn the key principles of data protection, as defined in the GDPR.
- 2. The end-users of the 5 LSPs who will be exposed to the IoT pilots. They should benefit from the game to better understand the risks related to IoT deployments and the means to mitigate these risks. The LSPs include very heterogeneous end users: farmers, event organisers, engineers, physicians, health carers, etc. We make the assumption that they do not necessarily have a superior education.

- 3. The large public in general. We make the assumption that they have different levels of education and not necessarily legal knowledge.