Law, standards, and compliance – group project – phases 2 and 3

Given the nature of our project (Working with LoRa devices, creating a secure network), the GDPR subjects do not necessarily fit into our scope. However, the packets sent contain data. This can be an aspect to be discussed for that matter.

GDPR stands for General Data Protection Regulation. It provides a set of standardized data protection laws regarding the processing of personal data across all member countries of the European Union.

AVG is the Dutch interpretation of the GDPR, given that every country can come up with its own specific guidelines. AVG governs the GDPR guidelines but also distributes its own in-depth guidelines. Therefore, the team should also study the particularities of the AVG.

It is also important to know that processing personal data can result into a fine. The team needs to be very careful with the data they are manipulating or data that they access in order to avoid such issues.

The team also needs to be careful about everything that can be classified as personal data, for which the GDPR rules apply. According to the definition, personal data is the data by which a person can be identified. The term personal data should be interpreted as broadly as possible when gathering information.

It is also important to categorize the personal data. It includes information such as religion, physical conditions, personal information in general. In order to be able to process it, an exception must apply. The Data Breach Notification Obligation includes personal data that contains race, ethnicity, political standings, religious beliefs, memberships, medical files, sexual preference, genetic research, and biometrical data. While working with data, the team must know what can be classified as personal data in case of a data breach, since they are obligated to notify the authorities. Reporting of data leaks is mandatory. The notification about data breaches needs to be sent to the Dutch Data Protection Authority.

Risk analysis is also an important step. The scope, nature and context of the data processing need to be considered before the start of the actual processing. An assessment of the impact needs to be done. This way, the risks are lowered when the team starts working.

While working with personal data, technical and organizational security measures are essential for a good workflow. Personal data needs to be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Integrity and Confidentiality parameters from the CIA diagram are to be taken into consideration.

Under normal circumstances, personal data is not being transmitted. However, the packets are stored in log files. The team should monitor the flow and in case personal data is received and decrypted by the system. This data must not be stored in the log file. The packets are transmitted through a secure gateway, so such occurrences should not take place. However, it is good to be cautious and train the group members to react properly to data leaks.