Association Européenne des Fabricants de Compteurs d'Eau et d'Energie Thermique
Europäische Vereinigung der Hersteller von Wasserzählern und Wärmezählern
European Association of Water Meters and Heat Meters Manufacturers

SECRETARIAT : AQUA
c/o Syndicat de la Mesure
Maison de la Mécanique
F 92038 PARIS LA DÉFENSE CEDEX
Tel : (+ 33) 01 43 34 76 80/81 - Telefax : (+ 33) 01 43 34 76 82/83

AQUA VIEW ON "EU Regulations on Data Protection 27.4.2016/25.5.2018 GDPR"

The following agreement is an AQUA guideline, which is not legally binding. Following this guideline does not assure that the users will be GDPR compliant. This is a recommendation only based on best practice.

This document is a working document and updated regularly by the AQUA COMMUNICATIONS WORKING GROUP.

AQUA AGREEMENT ON CEN/TC294 and ISO 27001 standards

AQUA agrees that for public acceptance of smart metering, suitable privacy and data protection safeguards need to be in place so that consumers are assured that their data are treated securely and that their privacy is not infringed. Personal data – as seen by AQUA – are defined as follows: data are personal when they can be tied to a person. For example, if data is transmitted in different moments i.e.: day X name, day Y consumptions, this is considered to be personal data and impacted by the regulation.

Aqua furthermore agrees that suitable privacy and data protection can be gained by applying published CEN/TC 294 standards, which takes into account the following Directives of the European Parliament: 2002/58/EC, 2006/24/EC and their corresponding evolution and as appropriate the General Data Protection Regulation (EU 2016/679).

In addition, AQUA agrees that suitable privacy and data protection can be gained by applying recommendations from ISO 27001 with its asset management, register, classification, labelling, control and its latest changes on:

- Information security in project management,
- Restrictions on software installation,
- Secure development policy,
- Secure system engineering principles,
- Secure development environment,
- System security testing,
- Information security policy for supplier relationships,
- Information and communication technology supply chain,
- Assessment of and decision on information security events,
- Response to information security incidents,
- Availability of information processing facilities.

AQUA AGREEMENT ON USE CASES

AQUA considerations for smart meter manufacturers generating data:

- Customers (utilities) who own the relationship with their end customers (consumer) and with the supervisory authority are behaving as data controllers as per the GDPR definition.
- Customers can be asked by end-consumers or an authority to demonstrate that they manage data in accordance with the rules and obligations established by GDPR.
- Companies that offer services using meter manufacturer's equipment can be considered as data processors. As a consequence, meter manufacturers should offer technologies that enable service companies to fulfil GDPR.
- For data transmission, several solutions exist to achieve data transmission. In accordance with the use case; e.g., mobile, fixed network, one way, two way, interoperable or proprietary. No matter what type of data transmission is used, data transmission has to follow GDPR rules.
- AQUA considers that selecting one of the protocols and encryption modes included in standards and published by the CEN/TC294 (wM-Bus, Mesh) and using individual device keys, allows to achieve compliance with GDPR requirements.
- For other solutions compliant to GDPR, manufacturers should be prepared to explain and justify to their customer how to assure security and privacy of the data generated and transferred.
- Attention has to be paid for the handling of encryption keys in general at the manufacturer up to the customer. The use of secure file transfer protocols and cryptography is recommended for ensuring entity authentication and the integrity and confidentiality of the keys material.

AQUA (in the advisory role) recommends to utilities and companies processing data to pay attention to the GDPR requirements and take into account the following considerations:

- Data regarding end user consumption, must be considered as personal data. Utilities will have to demonstrate over the full data processing chain that they have security controls in place to minimize the risk of privacy data exposure according to GDPR.
- For utilities it is recommended to follow the ISO 27001 standard for the identification of privacy sensitive assets, the analysis and treatment of security risks and the definition of appropriate controls for mitigation.
- All data collection shall be transparent and justified by a business interest of the utility to the end consumer
- For data analytic treatments, transparent and documented reasons must be available for data export. Data must be anonymized, if data analytics is conducted on materials that go beyond the legitimate need.
- Other specific rules or agreements might apply to improve efficiency and environmental protection e.g., for leakage detection
- Users of metering systems have to adjust internal processes in order to comply with GDPR
- International data transfer
    - Country specific rules might apply for example for transfer and storage of data

---

Version	Change	Note
1.5	First publication	Will be reviewed 2x per year
1.6	Typos	Corrected