AQUA's Position on the Implementation of the EU Data Act (Regulation (EU) 2023/2854)

Reference: Official Regulation Document

This document outlines the position of AQUA, the European Association of Water and Thermal Energy Meter Manufacturers, on the EU Data Act (Regulation (EU) 2023/2854).

Purpose and Scope

This white paper presents AQUA-Metering's interpretation of the EU Data Act in the context of utility metering. Its purpose is to clarify how the Act interacts with the legally regulated measurement environment and why direct access to metering data by home or flat owners may be restricted, conditioned, or routed through authorised parties where legal metrology, GDPR, cybersecurity, contractual roles, or utility obligations apply. The document focuses on the unified legal and technical treatment of metering data, the definition of legitimate users, and the constraints arising from legal metrology, data protection and cybersecurity obligations.

---

1. Introduction

The EU Data Act seeks to increase fairness and transparency in data access across connected products. Metering systems, however, operate within a long-standing regulatory structure that governs the accuracy, security and integrity of measurement data used for billing. Unlike general IoT devices, meters produce data that is part of a legally controlled process. Legally regulated billing and measurement data—consumption values, status messages, logs and metadata—forms a tightly controlled dataset that must remain protected throughout the entire measurement chain. Where the Data Act may additionally cover raw or pre-processed product data and relevant metadata that is readily available, a distinction should be drawn from inferred or derived data, which is generally outside the scope of the Data Act's access obligations.

In this setting, the Data Act must be applied in a way that respects legal metrology obligations, the contractual relationships in the metering ecosystem, and the unified security architecture used for all metering data.

---

2. Scope of the Data Act in Metering

While the Data Act broadly applies to connected products, it applies alongside—not in derogation of—other applicable Union and national requirements, including GDPR, privacy rules, legal metrology obligations, and cybersecurity requirements. The Data Act does not exclude metering from its scope but must be interpreted consistently with

these frameworks. For metering, this includes the Measuring Instruments Directive (MID), national calibration laws, GDPR and cybersecurity requirements. These frameworks define how data must be generated, transmitted and validated and determine who may access it.

In the regulated metering architectures considered by AQUA members, metering systems treat all generated data as part of the legally controlled measurement process. In these architectures, no internal categorisation typically exists that would allow selective release of specific data types without compromising the integrity of the measurement chain. The dataset is protected uniformly, and access is restricted to entities with a legal mandate.

---

3. Unified Security and Legal Status of Metering Data

Metering data is protected through a single security key hierarchy and a uniform communication architecture. This design is mandated by legal metrology, which requires tamper-evidence, traceability and consistency across all elements of the measurement process. Status data, logs and operational metadata are legally relevant because they influence validation and auditing.

GDPR further limits who may receive metering data. In typical utility-operated metering models, utilities act as data controllers with the legal basis for processing consumption information for billing. Where metering companies act as processors under such arrangements, direct disclosure of data to individuals would generally require controller authorisation or another valid legal basis. The specific controller and processor roles depend on the contractual and processing setup in each case. NIS2 cybersecurity obligations require that any additional access channels be assessed, secured, authorised, monitored, and aligned with applicable cybersecurity risk-management requirements.

Together, these frameworks result in a unified legal and security status for all metering data. Any subdivision or differentiated access is technically and legally constrained and should only be considered where it can be implemented without compromising metrological integrity, data protection, cybersecurity, or contractual responsibilities.

---

4. Why Open or Selective Interfaces Cannot Be Offered

In discussions around Recital (15) of the Data Act, it is important to distinguish clearly between **external interfaces that are already publicly standardised** and **internal data and processes that embody significant proprietary investment**. AQUA considers that existing metering interfaces already fulfil the transparency objectives of the Data Act without requiring any additional opening of interfaces or disclosure of internal data.

Metering devices provide established operating interfaces for data reading that follow **publicly available and widely adopted standards**, such as OMS, wMBus, LoRaWAN

and NB-IoT. These interfaces are designed specifically for operational data retrieval by authorised entities. Data transmitted via OMS is self-describing, meaning that the structure and semantics of the data are sufficiently defined by the standard itself and do not require additional metadata for interpretation. Where manufacturers use proprietary data elements, appropriate documentation can be made available to authorised parties without exposing internal system logic or compromising security.

In addition, local configuration or read-out interfaces, such as IrDA or NFC, are provided for commissioning, maintenance and service purposes. These interfaces comply with applicable regulatory frameworks, in particular the Radio Equipment Directive (RED) and the Cyber Resilience Act (CRA). They are not intended for continuous data extraction but for controlled, authenticated interactions in regulated operational contexts.

By contrast, **internal data within the meter or radio module**—including raw internal processing data, calibration parameters, internal states and control logic—reflects substantial financial investment and specialised technical know-how by manufacturers. These internal elements are essential to achieving the long-term stability, accuracy and reproducibility required by legal metrology. They ensure reliable operation over the full device lifetime and under all specified environmental conditions, and they underpin compliance with MID and harmonised standards.

Recital (15) of the Data Act recognises that protection of trade secrets and the results of significant investment are relevant considerations in determining data sharing obligations. For inferred, derived, proprietary, or security-sensitive internal meter data that is not readily available as raw or pre-processed product output, these protections are directly relevant and should be assessed on a product-specific basis. Where such internal data constitutes proprietary design or manufacturing expertise inseparable from the meter's core function, there is no obligation under the Data Act to disclose it or to provide access beyond the already standardised operating interfaces. This conclusion does not apply categorically to all data generated by metering products; raw or pre-processed product data and relevant metadata that is readily available may remain within scope of the Data Act's access provisions.

Taken together, the existence of open, standardised operating interfaces combined with the protected nature of internal meter data demonstrates that the objectives of Recital (15) are already met in the metering sector. No further opening of interfaces or exposure of internal data is required or justified.

---

5. Interpretation of "User" in the Metering Context

The Data Act defines the user broadly as a natural or legal person who owns, rents or leases a connected product or receives a related service. In the metering context, AQUA's position is that the relevant user is typically the utility or metering point operator, who procures, operates and manages metering systems and holds the legal responsibilities for data processing, billing and customer communication. Whether

household occupants may qualify as users under the Data Act requires a case-by-case assessment of ownership, contractual role, legal entitlement, and the applicable national metering framework. In typical utility-operated models, household occupants do not have a direct contractual relationship with the metering company enabling direct data provision.

Accordingly, AQUA's position is that in typical utility-operated metering models, the Data Act access rights accrue primarily to utilities or other entities legally responsible for metering operations. This interpretation is subject to the specific ownership, rental or lease arrangements, related-service context, and applicable national metering law that may apply in individual cases.

---

6. Interoperability and Standards

AQUA supports interoperability efforts under the Data Act where they are compatible with metering regulations. Standards must respect the unified legal and security status of metering data and avoid requirements that would compromise metrological control or create new access pathways. Harmonisation should strengthen secure data exchange between utilities and metering companies without altering established responsibilities.

---

7. Conclusions

The Data Act introduces new expectations for data accessibility that must be assessed within the constraints of legal metrology, GDPR, cybersecurity obligations, contractual roles, and the applicable national metering framework. In the regulated metering architectures considered by AQUA members, the division of metering data into categories for different recipients and the provision of open or selective interfaces to household occupants raise significant legal and technical concerns. Utilities are typically the legitimate users of metering devices in these models and remain responsible for communicating consumption information to consumers. The appropriate access framework for each deployment should be assessed on the basis of the specific legal, contractual, and technical circumstances involved.

AQUA supports a consistent European approach that aligns the Data Act with existing metering legislation while maintaining the integrity and security of utility billing processes.

About AQUA

AQUA primarily represents family-owned small and medium-sized enterprises that provide products and solutions for critical infrastructure and energy efficiency across Europe.

Version: 1.0

By presenting this position, AQUA aims to contribute to the development of a robust regulatory environment that supports innovation, cybersecurity, and market harmonization within the EU.

AQUA View on the EU Data Act (Regulation (EU) 2023/2854)