

Article

Towards Energy Efficiency: A Framework for Measuring, Reporting and Verifying Energy Data from Smart Buildings

Julia Köhlke ^{1,*}, Anna Brüning-Pfeiffer ², Viktor Dmitriyev ¹, Franziska Tucci ² and Jad Asswad ¹ 

¹ OFFIS e.V.—Institute for Information Technology, 26121 Oldenburg, Germany

² Berliner Energieagentur GmbH, 10623 Berlin, Germany

* Correspondence: julia.koehlke@offis.de

Abstract

Measurement, Reporting and Verification (MRV) concepts have emerged as a means for reviewing and ensuring the effectiveness of energy efficiency measures (EEMs) in smart buildings. Nevertheless, high technological and regulatory demands imposed by the Energy Efficiency Directive, Article 8 (EED 8), result in limited adaptation, which makes the transition of the MRV concept into a practically applied framework a challenging endeavor. A significant concern lies in ensuring data integrity, accuracy and transparency throughout the entire adaptation and implementation process of the MRV concept. This study addresses these challenges by developing and evaluating a structured MRV framework tailored to smart building environments. The MRV framework design was tested in a real-world use case in Berlin, demonstrating its applicability for measuring, reporting and verifying energy efficiency data from smart buildings. The results confirmed the applicability of the approach, while also revealing persistent barriers related to data sovereignty, security and interoperability. Ensuring trust, transparency and long-term data accessibility requires robust governance structures and alignment with legal and ethical standards. Future work will focus on scaling the MRV framework to additional sectors and refining mechanisms for secure data sharing and automated verification.

Keywords: measurement, reporting and verification (MRV); energy efficiency; smart buildings; EED 8; data sovereignty

1. Introduction

Energy efficiency (EE) is a key objective of numerous European Union (EU) policies and was also embedded in the Paris Agreement of 2015 to establish a smarter and more sustainable energy grid [1]. EE also plays an important role in smart buildings, which are designed to reduce energy consumption relative to conventional buildings while maintaining an equivalent level of occupant comfort and service quality. Accordingly, smart buildings are engineered to seamlessly incorporate various features, including the ability to adapt to climatic conditions, respond dynamically to energy grid demands, and align with user preferences. Additionally, they include advanced capabilities for continuous monitoring and efficient supervision, ensuring optimal performance and sustainability [2]. In the context of smart buildings, this objective is primarily achieved through the enhancement of design, construction, operation and maintenance across the entire life cycle [3], complemented by the integration of renewable energy sources and smart technologies [4]. Particularly in the context of § 14a of the German Energy Industry Act (EnWG), the trace-



Academic Editor:
Francesco Minichiello

Received: 15 August 2025
Revised: 13 January 2026
Accepted: 22 January 2026
Published: 13 February 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

ability of energy efficiency with the help of measurement, reporting, and verification (MRV) in smart buildings is becoming increasingly important.

Article 8 of the EU's Energy Efficiency Directive (EED 8) promotes the implementation of new energy efficiency measures (EEMs) in smart buildings across all European member states, with the aim of supporting the EU's climate and energy objectives. The European Commission (EC) plays a central role in driving the implementation of these measures by, for example, providing the legislative framework and policy developments [5]. The EC has mandated that these EEMs be reported to the EC and incorporated into each European member state's National Energy Efficiency Action Plan (NEEAP). NEEAPs comprise a broad set of policy instruments, including Energy Efficiency Obligation Schemes, dedicated funds and subsidy mechanisms, taxation measures, regulatory actions and voluntary agreements. In addition to the EC, Schmidt et al. emphasize the role of key performance indicators (KPIs). These KPIs play a vital role in demonstrating the EEMs to other third parties, such as consumers, enabling them to monitor their energy performance [6].

The Measurement, Reporting and Verification (MRV) concept shows divergent representations in the literature. The International Performance Measurement and Verification Protocol (IPMVP) introduced and defined the concept of Measurement and Verification (M&V), while the Bali Action Plan, adopted at the Conference of Parties 13 (COP 13), formulated the concept of MRV. Both were introduced in 2007 with the aim of meeting regulatory requirements. This indicates parallel development of the concept, with emphasis on different aspects. The IPMVP defines M&V as "the process of planning, measuring, collecting, and analyzing data to verify and report energy savings resulting from the implementation of EEM in one or more facilities" [7]. The M&V concept focuses on the Measurement and Verification of energy savings and greenhouse gases. Therefore, the implementation of M&V mainly focuses on the project or installation level to verify the actual energy savings, not on further processing or reporting to various stakeholders. The developed Measurement, Reporting and Verification (MRV) concept includes an additional level of reporting, incorporating data management and the provision of EE data to other stakeholders. Hence, MRV considers a broader conceptual process, encompassing further steps of reporting and international verification related to emission reductions, climate actions or resource management.

1.1. Research Subject and Challenge

The integration of EEM into smart buildings, together with the associated increase in information and communications technology (ICT), requires more data to be exchanged. This poses significant challenges in terms of regulatory requirements and coordinating the various actors involved [8]. The use of data from smart buildings often conflicts with data sovereignty and the need to protect individuals and organizations from data leaks or unauthorized access [9]. At the same time, the existing literature remains inconsistent on handling MRV data [10], leading to uncertainties in implementing MRV frameworks in today's organizations. The critical management of such data, as well as the high demands of data sovereignty, interoperability and other regulatory obligations, make the endeavor of MRV implementation highly complex. Conversely, the implementation of an MRV framework constitutes a critical element in ensuring the provision of essential data and transparency, thereby facilitating effective actions in terms of EE.

Current practices for implementing MRV concepts that should display EEM often reveal incompatibility between the current guidelines proposed by the EC and the organization's deployment strategies. Although trustworthy measurements are imperative, e.g., for investors or regulators of cost-efficient programs [11], prevailing practices frequently fall short in terms of the necessary level of trustworthiness. Thus, calculations are often

unreliable due to the absence of robust verification methodologies. This results in high uncertainty with regard to the use of MRV measures for EE. At the same time, an economic concept that motivates or incentives consumers or tenants to adopt actions beneficial to EE remains undeveloped. Altogether, a gap can be observed between the regulatory requirements of the EC and the actual implementation of a holistic MRV framework on the part of the organizational stakeholders. Although some MRV concepts have been developed for handling EE, there are only few real-world implementations of MRV frameworks that are fully compliant with regulatory and technological requirements. This paper therefore provides navigation for implementing an MRV framework under Article 8 of EED in practice. In light of this background, the following question is raised: How can the MRV concept from the EED 8 regulation be developed into an actionable framework for organizational implementation and improved energy efficiency in smart buildings?

1.2. Objectives and Structure

The paper presents an MRV framework for smart buildings that translates the demands from EED 8 regulations into practice. For this purpose, we present a real-world use case and subject it to a feasibility analysis in accordance with EED 8 specifications. In the use case, we also introduce a new approach to incentivizing tenants to adopt EE measures. The relevance of translating the MRV framework into practice is evident in the need to ensure compliance with regulations, enable transparency and accountability, and facilitate data-driven decision making and the realization of sustainable goals within smart buildings.

The present paper begins with an introductory chapter, delineating the research topic, objectives and the research question. Subsequently, Section 2 furnishes pertinent background information to contextualize the research topic and identify gaps in the literature. The literature background includes MRV and EED 8 in the energy domain, interoperability, data sovereignty and the Smart Grid architecture model. Section 3 offers an overview of the design options for the MRV framework, including general conditions as well as existing MRV concepts from the literature. Section 4 describes a use case from a European project that is currently implementing an MRV framework in buildings using different technological solutions. Finally, Section 5 provides a discussion and Section 6 summarizes the research findings and their implications, as well as recommendations for future research.

2. Background

2.1. Overview of MRV and EED 8

In recent years, the term “MRV” has been increasingly used in the energy sector, where initiatives aim to incorporate a range of EEMs and tools to make buildings greener and smarter. These EEMs, however, often have different intervention scales and objectives, leading to differences in the MRV concept and its scope [12]. In general, MRV concepts are used to increase energy savings, document financial transactions, improve energy-efficiency projects and engineering designs, as well as enhance the operation and maintenance of facilities [7]. In addition, MRV concepts can be applied at the organizational, national or international levels, such as in Nationally Appropriate Mitigation Actions (NAMAs) [12]. At the organizational level, an MRV concept aims to analyze emission data from facilities, prepare information for the relevant stakeholders or assess climate risks and opportunities. From a national perspective, the data and information collected as part of MRV are gathered with the aim of ensuring compliance and the formulation of new policies within a country [12]. With a view to the future growth of sustainability reporting at an international level, MRV is a key component of any European climate policy or action aimed at reducing emissions and enhancing transparency and accountability. In this sense, MRV facilitates

tracking the progress and impact of EEMs, which account for a significant share of global emissions [13].

The MRV term was originally introduced in the Bali Action Plan, adopted at Conference of Parties 13 (COP 13) in 2007, which aimed to strengthen mitigation in climate change action at the national and international levels. In this Bali Action Plan, MRV was introduced as a principle that comprised national communications, reports and international analysis regarding EE [14]. A few years after introducing the Bali Action Plan, the Energy Efficiency Directive (EED) was adopted by the EU in 2012 to create a legally binding act to measure EE across all member states of the EU [15]. The agreement was established to set out the EU's climate change targets and energy policy. Article EED 8 (earlier EED 7) demands that all European member states should achieve a cumulative amount of energy savings and should implement Energy Efficiency Obligation Schemes (EEOs) or Alternative Policy Measures (APMs) to reduce energy consumption. The Measurement and Verification part was already an integral part of EED 8 to ensure the transparency, accountability and credibility of the energy savings. Specifically, Article 8b of the EED states that a system of measurement, verification and control must be set up to ensure that the energy savings claimed by EEOs or APMs are actually achieved. The MRV system to be developed has to include clear and unambiguous definitions of eligible EE improvement measures and actions. Furthermore, EED 8 suggests methodologies for the calculation or estimation of energy savings based on harmonized principles and methods. For example, it provides some quality standards for the installation, operation and maintenance of the measures and actions. Additionally, it also provides guidance and support for European member states to set up and implement MRV systems. These are examples of the principles and methods used to calculate or estimate energy savings. They offer a common framework for reporting on EEOs or APMs and technical support and capacity-building tools for European member states on MRV issues. It can be concluded that EED 8 is therefore closely linked to the concept of MRV, as it outlines the initial steps for its implementation within the participating organization. However, the EED does not provide any clear information about which technological design option should be used for the reporting part. To conclude, MRV has become a recognized framework at both international and national levels for measuring EE in smart buildings [12]. Although it has evolved considerably over time, it still faces limitations, particularly with respect to reporting practices.

The three building blocks of MRV are described as follows in today's literature: While "measurement" is related to the data and information relevant to emissions and its quantification and visualization of EEM, "reporting" is about the data processing of energy savings actions, and "verification" is about the control mechanisms that are needed for examining the individual energy-saving actions [7]. The main target group of MRV is often public bodies, individual persons or companies; however, beneficiaries or obligated parties that are involved in performing EEM are also targeted. Similarly, there are MRV regulations for different sectors: MRV4EU ETS (Emissions Trading System), MRV4Regulation for maritime transport, or EED 7 with MRV4Smart Buildings, e.g., [12].

Measurement: MRV is based on a step-by-step process to measure, report and verify the amount of greenhouse gas emissions. The first step is the "measurement," which can comprise different approaches for setting baselines and measuring emissions reductions. It represents one of the initial steps of MRV, as measurements are essential for quantifying savings and making them visible to address their impact. Measurement can be performed by metering and modeling or by combining both. The measurement should therefore provide a first basis of data that is necessary for introducing effective measures and informing future policy decisions. The metering part can take place with the help of smart meters that aim to record electricity consumption at the customer's premises. As a result,

consumers will not only have more control over their consumption, but the distribution system operator (DSO) or the energy service company (ESCO) will be able to manage electricity more effectively. In this sense, ESCOs can be responsible for delivering energy savings through the implementation of energy efficiency projects. MRV systems ensure that the energy savings claimed by ESCOs are measured, reported and verified accurately.

Reporting: Once the measurements have been conducted, the next step is to carry out the reporting. However, while the need for Measurement and Verification has already been mentioned in EED 8, it is evident that the reporting component has not yet consistently been incorporated in prior discussions, nor has it been delineated in sufficient detail. Within MRV concepts, reporting is typically defined as the data management or submission mechanism by which energy savings are systematically conveyed to relevant parties. Following the measurement of energy savings, this reporting step is to present or visualize these savings, as well as to derive predefined KPIs. The data-processing stage also includes the submission or documentation of energy savings to the accredited parties. This is performed with the intention of creating transparency for the organization's obligations to report on efforts to avoid or remove harmful emissions. The reporting results will be finally used for the last step, verification.

Verification: The final verification step involves a control mechanism that is intended to check whether the measurements have been carried out accurately and that the data were transmitted correctly. It should also serve as a control mechanism for the data. The verification part therefore guarantees that the transmitted data are secure, robust, transparent, consistent and accurate, and that no errors have occurred during measurement or reporting. The verification step often takes place by a party that is not included in either of the previous processes.

2.2. MRV Approaches in Today's State of Research

Taken together, for EE buildings, MRV requires a careful design and implementation that considers the specific context, needs and objectives of each intervention, as well as the best practices and lessons learned from existing experiences. To identify current best practices in research and practice for the different building blocks of an MRV system in the application area of EE in smart buildings, a systematic literature review has been conducted to identify the current state-of-the-art on "*how to design MRV systems*." The literature review (see Table 1) shows that MRV was presented in different papers. It is striking that the reporting part has not always been integrated in the literature. This again highlights the research gap on data management in MRV and its organization between different actors.

The review of the existing MRV frameworks and related documentation reveals a diverse landscape of methodologies addressing energy efficiency, climate mitigation, and data governance. The analysis covers documents published between 2013 and 2022, reflecting the gradual evolution from sector-specific energy performance protocols toward more integrated, cross-domain MRV systems.

Early initiatives, such as the Energy Efficiency Directive (EED) and its implementing articles, e.g. EED 7 (today EED 8), established the foundational legal and methodological principles for monitoring and verifying energy savings within the EU. Subsequent documents, such as SENSEI (2021) and ENSMOV (2020), extended these concepts by providing detailed guidance for designing and implementing performance-based MRV schemes. These frameworks increasingly emphasize the reproducibility, transparency and harmonization of metrics across jurisdictions. The International Energy Efficiency Protocol (IEECP, 2021) and the International Performance Measurement and Verification Protocol (IPMVP, 2016; 2020) remain cornerstones for the definition of standardized procedures in energy performance contracting and carbon mitigation. They serve as reference models for developing consis-

tent monitoring and reporting procedures across projects and sectors. Moreover, recent developments, such as the EENSIGHT project (2022), illustrate the growing potential of artificial intelligence and machine learning to enhance the accuracy and scalability of MRV processes, particularly in predicting and benchmarking building energy usage.

Table 1. Literature Review on Measurement, Reporting and Verification (MRV).

Acronym	Documents	Year	Domain		Aspects		
			Energy	Measurement	Reporting	Verification	Payment
IEEFP	International Energy Financing Protocol (IEEFP) [16]	2021	X		X		X
ENSMOV	Setting up an MRV system—Step by step guidance [17]	2021	X	X	X	X	
ENSMOV	Cost Effectiveness for Monitoring, Reporting and Verification (Article 7 EED) [18]	2020	X	X		X	
EED 7 (today_EED 8)	Evaluation of Fiscal Measures in the National Policies and Methodologies to Implement Article 7 of the Energy Efficiency Directive [19]	2016	X	X		X	
	The Energy Efficiency Directive—Article 7 EED [20]	2020	X	X	X	X	
	Guidance note on Directive 2012/27/EU on energy efficiency, amending Directives 2009/125/EC and 2010/30/EC, and repealing Directives 2004/8/EC and 2006/32/EC Article 7: Energy Efficiency Obligation Schemes	2013	X	X	X	X	
	Plan for implementation of Article 7 of the Energy Efficiency Directive	2013	X	X	X	X	
SENSEI	D5.2 Guidelines for the design of P4P schemes [21]	2022	X	X		X	X
	D7.2 Methods for the dynamic Measurement and Verification of energy savings [22]	2021	X	X		X	
	D8.2 Consolidated services and technical standards catalogue	2021	X	X		X	
FEMP	M&V Guidelines: Measurement and Verification for Performance-Based Contracts Version 4.0 [23]	2015	X	X		X	X
EENSIGHT	Can we make ML models to predict a building's energy usage?	2022	X			X	
IPMVP	International Performance Measurement and Verification Protocol (IPMVP)—Core Concepts [7]	2022	X	X		X	
	MRV 101: Understanding Measurement, Reporting, and Verification of climate change mitigation	2016	X	X	X	X	
	From strategy to deliver: Measuring, Reporting, Verification of Urban Low Emission Development	2016	X	X	X	X	
	Parameters for Monitoring, Reporting and Verification of Article 7 Energy Efficiency Directive	2020	X	X	X	X	

Notably, a significant portion of these studies emphasize Measurement and Verification, while the aspect of Reporting remains unexplored. Consequently, significant disparities exist in data handling practices among various organizations. The limited attention given to data reporting in previous studies indicates the absence of established best practices for its implementation. To address this gap, we propose three potential

design options for the implementation of MRV based on emerging technologies, which are presented in the following Section 3.

2.3. Data Sovereignty

Data sovereignty is a cornerstone of the European data strategy, with recent European laws and regulations further strengthening associated rights and control mechanisms. EU law applies to data collected in the EU and/or to data subjects in the EU [24]. As data sovereignty has become a central element of contemporary data governance debates, it represents key consideration in the development, adaption, and deployment of new data technologies [25]. In the face of increasing digitization, data sovereignty is becoming indispensable given the growing flows of data and the complexities involved in handling them between a growing number of organizations. Compliance with General Data Protection Regulation (GDPR) also underscores the importance of data sovereignty to guarantee privacy and security of personal data [26]. From an MRV perspective, data sovereignty holds particular relevance in determining who has access to specific data and where that data should be stored.

Dealing responsibly with data is a major challenge today and faces the dilemma that, on the one hand, the use of personal data can be beneficial in the customization of many services and the development of novel digital products. On the other hand, it imposes a number of crucial risks, such as the loss or misuse of personal data. Against this backdrop, data sovereignty signifies the principle that data generally remains with the owners of the data [27]. In particular, the widespread use of domestic or foreign cloud solutions for data storage has further intensified the issues of data sovereignty, as the governance of data is in the hands of the cloud owners. Most authors of this discourse understand data sovereignty as the authority to make binding decisions grounded in national arrangements or international governance. It is therefore often explained as the “control of data flows via national jurisdiction” [27]. Data sovereignty therefore relates to the self-determination of organizations as well as individuals in terms of the use of their data [28].

However, the concept of data sovereignty has received limited theoretical discussion in the literature, resulting in a variety of different definitions and interpretations of what data sovereignty actually is and how it can be defined. According to [29], “data sovereignty refers to forms of independence, control, and autonomy over digital data, emphasizing the need for users to maintain control without reliance on central authorities. It is crucial for ensuring privacy and security in digital identity management”. European legislation and regulations addressing data sovereignty are currently expanding. This development reflects the growing need for data to be processed and exchanged through increasingly automated and semi-automated mechanisms, while ensuring compliance with diverse contractual obligations and legal requirements across jurisdiction [28]. These regulatory developments, which increasingly bind data to the territorial jurisdiction of the respective organizations and restrict cross-border transfers, indicated a growing prominence of the concept “alliance-driven data ecosystems” is becoming increasingly popular [28]. However, the concept of data sovereignty also entails some complexities, particularly with regard to privacy, security, trust, and ethics [30]. Hence, data sovereignty therefore raises issues, such as how and where data are stored, processed, and transmitted, as well as which data elements need to be secured [30].

One of the main complexities of data sovereignty can be observed in the context of *data privacy*. Data privacy is often understood as informational friction, defined as “the forces that oppose the flow of information” [31]. Hence, privacy is often regarded not only as a protective concept but also as a constraining one [25]. However, data sovereignty is in conflict with the restrictive part of data sharing and the expression of solidarity

due to the common commitment to the sharing of data [25]. This is also referred to as the privacy paradox. Another complexity is also given by governments' access to data as well as the regulations established by these governments. In general, the degree to which governments feel obligated to protect the privacy of data varies across different nations. Many governments are therefore concerned about citizens' data being accessible to governments of foreign countries. Contrarily, the capability of governments to access personal data held by other organizations is also addressed within this aspect.

Another aspect of data sovereignty is *security*, which is necessary to maintain trust among different organizations. Data security aims to assure the identification of stakeholders, but also to secure all data exchanges and communications [32]. It is therefore a part of common practice to protect data and information from unauthorized access, as well as from corruption or unwanted data thefts.

Trust is another complexity of data sovereignty and refers to a sense of confidence that data will be used in an accurate way. This entails the implementation of cyber-security measures to safeguard data, thereby ensuring transparency throughout the data usage process. Trust is generally a highly necessary but complex aspect of data sovereignty, as it always involves a dependency from one party to another, which can lead to an opportunistic relationship between these parties [33]. The five Ts of trust stand for the principles of transparency, thoroughness, timeliness, trending and telling. The transparency of data is therefore a crucial aspect of trust, which can be defined as "the ability of the subject to effectively gain access to all information related to data used in processes and decisions that affect the subject" [34]. Data transparency should be available throughout the entire data pipeline from the origin to its usage and destruction [35] in order to guarantee trust between organizations regarding the data.

Finally, *ethics* play a crucial part when debating data sovereignty due to the increasing demand for an ethical use of data. It is imperative to acknowledge that ethical aspects extend beyond the aforementioned aspects and require dedicated discussion. Floridi and Taddeo [31] assume that data ethics is particularly concerned with moral challenges related to data sovereignty, specifically with regard to data processing, as well as generation and dissemination [36].

The aforementioned challenges underscore the necessity to clearly define the conditions required to safeguard data owners' sovereignty. Consequently, the development and implementation of a data sovereignty-compliant MRV framework necessitate the fulfillment of specific requirements. Accordingly, these requirements must address data sovereignty from ethical, legal, technical, and case-specific perspectives, while also ensuring interoperability among heterogeneous actors and diverse MRV systems. In the light of these requirements, a set of suitable procedures, recommendations, and functionalities could be derived. These could include consent procedures for tenants, data anonymization and aggregation steps, retention periods, rights to erasure in relation to immutable ledgers, and the jurisdiction and contractual controls governing any cloud components.

2.4. Interoperability and the Smart Grid Architecture Model (SGAM)

Beyond data sovereignty, interoperability constitutes a central component of the MRV framework. The SGAM provides an architecture framework that supports the systematic identification and evaluation of design options for the efficient exchange of MRV data among different stakeholders [37]. The SGAM has been established in the smart grid coordination group under the European mandate M/490 and is a framework used in the field of energy systems and smart grids. While the original aim was to uncover gaps in smart grid standardization, it has since evolved into an established framework within the requirements engineering of smart grids. On the one hand, the SGAM is able to

map the interoperability between different systems and, on the other hand, it ensures compliance with data sovereignty across several systems in actors in the smart grid. It enhances the design and analysis of smart grid architectures by providing a structured approach to understanding the various components and their interactions. In general, the SGAM serves as a common language for describing and comparing smart grid use cases, promoting efficient energy management and enhancing communication in the entire smart grid ecosystem [37]. Similarly, the SGAM can be designed using the standardized IEC 62559-2 [38] use case template. The template is intended to guide all stakeholders and establish a consistent structure for the use case [37]. Its purpose is to enable a uniform and systematically organized description of the use cases [37].

The SGAM comprises five interoperability layers: the business, function, information, communication, and component layers. On the X-axis of the SGAM are the different domains of the energy system from bulk generation to transmission, distribution, distributed energy resources and finally customer premises [37]. The Y-axis comprises the different zones that replicate the automation pyramid from process, field, station, operation, enterprise and market. The IEC 62559-2 standard delineates a use case template, referred to as the “Word template,” which consists of eight distinct sections. This template is designed to facilitate the description of the SGAM [37]. It is often the foundation for the development of SGAM and includes more details for specific use cases. To conclude, SGAM should enable interoperability in order to support efficient communication, to enhance system integration, to achieve diverse business goals, to achieve technical comparability, and to make systems more adaptable to each other [37].

3. Systematic Design Options for an MRV Framework

After outlining the fundamentals of MRV and introducing key concepts, including data sovereignty and interoperability, this section proceeds to present the design of an MRV framework for practical implementation. Building on the core principles and objectives established in Section 2, the following designs explore different ways the framework can be structured, organized and applied. Rather than prescribing a single solution, this Section outlines alternative approaches that address the same underlying concept from distinct architectural and functional perspectives. Together, they underpin the assessment the framework’s effectiveness and support its implementation in the subsequent use case. Likewise, SGAM functions as a cohesive bridge, enabling seamless integration into an interoperable landscape. It provides a consistent visualization of different design options and clarifies the interaction between MRV components and existing energy-system architectures. This approach is intended to create a holistic picture that informs and guides decision-making.

Developing an MRV framework for practical implementation necessitates a step-by-step process to ensure the selection of an appropriate design solution. This process is based on [21], which considers and combines technology with a business perspective. For each building block (M); (R); (V) of the framework, specific questions are posed to identify the most suitable implementation within MRV framework. This Section 3 therefore offers guidance on identifying different design options. It presents the design conditions and requirements, outlines best practices from the literature for using an MRV framework and provides a brief introduction to the various technologies.

3.1. General Conditions and Requirements

Since MRV frameworks for EE in smart buildings have not yet been widely implemented in practice, despite growing demand driven by governmental and EU regulatory requirements, early-stage design considerations are of particular importance. However, the

availability and quality of data collected in smart buildings remain insufficient in many cases. Historically, access to high-resolution metering data has been limited; however, this constraint is gradually being alleviated through the expanding deployment of smart meter gateways.

Pursuant to the German §14a EnWG, an increase in available data is anticipated, which necessitates the selection of an appropriate MRV design option. At the same time, selecting the right implementation strategy is becoming increasingly complex, particularly in light of the specific framework conditions and requirements within the application domain. Three critical considerations pertinent to the deployment of EE in smart buildings must be addressed, namely EED 8-compliance, interoperability and data sovereignty.

EED 8-compliance: EED 8 requires the establishment of systems that are able to monitor, report and verify the energy savings; in other words, it requires systems that can collect and process data regarding energy consumption. At the same time, data sovereignty must be assured when transparent, trusted and verifiable reporting is established. **Data Sovereignty:** Currently, European laws and regulations are expanding upon the rights as well as controls of data sovereignty. Data sovereignty is “the ability of individuals, organizations, and governments to have control over their data and exercise their rights on the data, including its collection, storage, sharing, and use by others.”

Interoperability: As the technical solutions applied within smart buildings are heterogeneous in nature and the deployment of MRV-solution at a large scale requires the participation of multiple independent stakeholders in different roles, the (syntactical, semantic and pragmatic) interoperability between the independent solutions is rarely given. The design options should therefore include different important standards within the area of smart buildings and smart grids, such as ISO 50001, ISO 19650 (BIM) or IEC 62939. As a result, a high level of institutional coordination is required to achieve interoperability.

Overall, the analysis showed that it is necessary to provide data not only to various regulatory bodies but also to consumers, ESCOs and other relevant entities. However, there is a significant gap in terms of data reporting between different stakeholders. Practical experiences show that so far there are few examples of data management in the context of MRV frameworks.

3.2. Technology Assessment as Design Options

The technology assessment is based on different questions that can be asked in the building blocks measurement, verification and reporting within the framework. Figure 1 shows the different questions for measurement, reporting and verification. A series of questions were formulated for these three steps.



Figure 1. Design considerations for MRV.

To determine how an MRV framework can be optimally implemented while taking EED 8-compliance, data sovereignty and interoperability into account, this study examines three technical design options at this stage: cloud solutions, blockchains and data spaces. Although cloud solutions represent the most widely adopted technology for data management today, blockchain technology has been employed for data management purposes for several years. In recent years, data spaces have also emerged as a novel alternative for the management and governance of data. Simultaneously, the global rise in data storage and processing heightens risks to data protection and security, as well as the dependency on providers. However, all three of these examined technologies have different benefits and drawbacks and are best applied for different use cases. To date, a comprehensive analysis of the design options that can be integrated into an MRV system has not been conducted. Therefore, this section presents an overview of the available technologies that could be relevant for the implementation of an MRV framework.

Cloud technology is the management of data over the internet, particularly independent of the kind of device [39]. In most cases, the cloud provides various services in the form of servers, applications and data storage. Access is usually easy for different users because the infrastructure can be flexibly customized and resources can therefore be flexibly expanded [39].

Blockchain was developed in the 1990s and has evolved very quickly since then [39]. It is a decentralized database consisting of a chain of individual blocks that are linked to each other. Each block contains various transactions and has a hash value that originates from the previous block. In this sense, the hash allows the blocks to be arranged in the correct order. Each node saves a copy of the blockchain and validates the transactions before they are recorded. This makes the blockchain not only transparent, but also very secure from attacks [39].

Data spaces are the latest technology that can be used to manage data between heterogeneous organizations. The concept seeks to establish an integrated and sovereign data ecosystem among various organizations, each with unique conditions for managing their data [40]. In general, only certified organizations have access to the data space, which is why certain rules are set by the certification process. This means that access to the data space is always restricted, although companies of all sizes are eligible to participate [41].

The selection of appropriate technologies for the MRV framework is guided by key considerations related to data sovereignty. In particular, blockchain technology will be examined as a possible enabler for the reporting part within the MRV framework of the following Berlin use case, and its role will be illustrated within an overall architecture model. Blockchain is considered due to its inherent characteristics, such as immutability, auditability, decentralization and automated execution via smart contracts, which directly address persistent challenges in MRV concepts. To systematically assess the integration of blockchain, the SGAM is utilized as the guiding methodological framework.

4. Use Case: Maximizing Energy Efficiency in a Berlin Residential Building

This chapter explores a real-world development and testing of an MRV framework through a use case based in Berlin, Germany. The use case highlights the potential of technological innovations, based on digital solutions, to drive energy efficiency in urban residential complexes. The use case, titled “Energy Performance Contracting with Pay4Performance Guarantees” stems from the European project Innovative Energy (Efficiency) Service Models for Sector Integration via Blockchain (InEEExS). The core concept of the project is the design, development and deployment of integrated energy services across sectors and carriers, using smart contracts and tokens to facilitate energy saving and energy efficiency while relaying data in a public blockchain and empowering coop-

eration among market segments and actors. It focuses on developing innovative energy smart contracts that are used as foundation to incentivize tenants to optimize solar energy self-consumption.

The core idea is to integrate renewable energy systems with user-centric digital applications to enhance and improve energy consumption behavior. The use case is developed within a residential complex in Berlin consisting of five buildings. The solar systems on the building rooftops are operated by an ESCO, which also takes care of the electricity contracts of the tenants. An ESCO is a service company that specializes in offering and implementing energy-efficiency-related projects for its customers. The role of ESCOs is to plan, finance, implement and often operate energy-saving measures.

Within each building, solar power is generated by rooftop solar power (PV) systems, which have been designed to be used in residential units. Besides solar panels, each building also includes and operates an electric vehicle (EV) charging station within its complex. The total capacity of the five solar systems is 99 kWp. Currently, only 60–70 percent of the generated solar power is utilized on-site, with the remainder fed into the energy grid. The project seeks to maximize self-consumption by using a mobile app that provides real-time data visualization of one's energy consumption and the current production of the rooftop solar plant. Usage of the mobile app should enable residents to adapt their energy usage patterns and align them with peak solar production periods. As an example, Figure 2 shows the data of the solar system's production in June 2025. In Figure 3, the solar production over the course of one day, June 2025, is displayed. The same data are provided in the mobile app and transferred in the form of calculated KPIs down to the minute into the blockchain. These KPIs are used to estimate and measure performance of solar quota, solar utilization, and solar quota in an EV charge. The solar quota KPI is the solar quota for a building, with the ratio of PV energy consumption per building. The solar utilization KPI is the efficiency of PV capacity utilization by tenants. The EV solar quota KPI is a ratio of energy from PV consumption per EV.

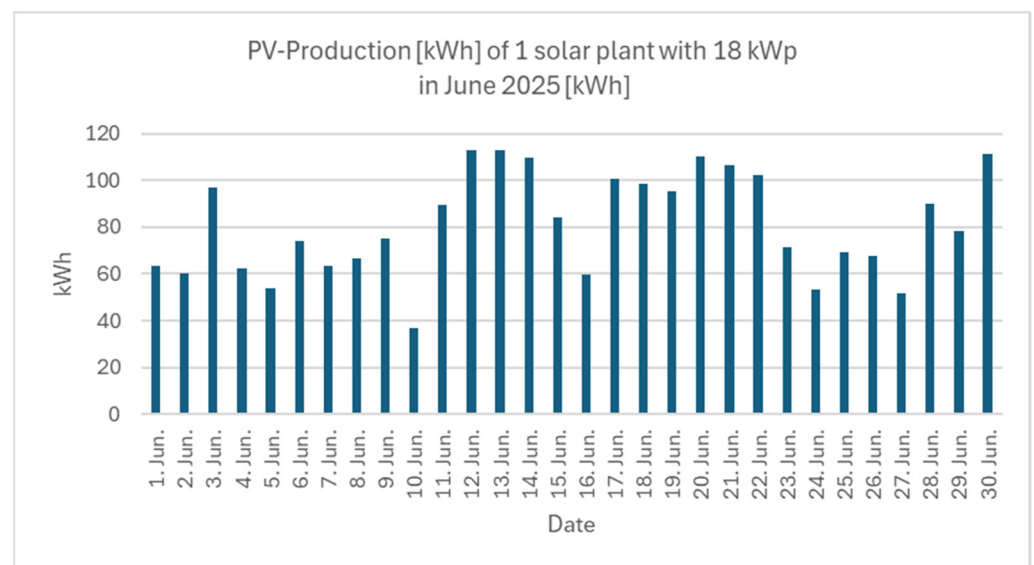


Figure 2. Overview of solar energy feed-in over June 2025.

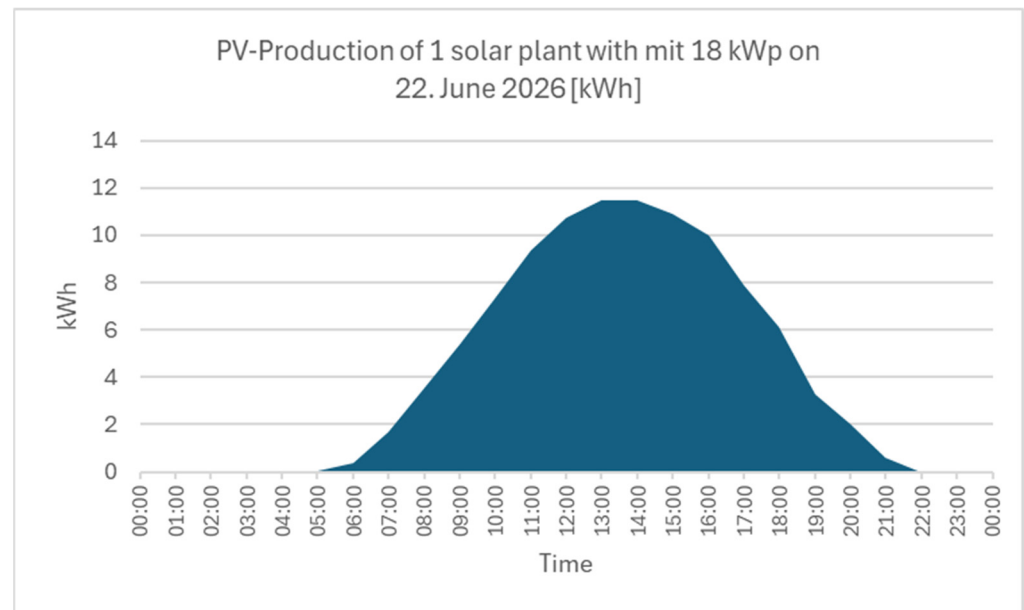


Figure 3. Example of daily production of solar energy on a day in June 2025.

The mobile app facilitates interactions between users and energy systems by providing actionable insights on how residents can act in order to optimize their own energy consumption. Additionally, the gathered data could be used as a foundation for future business models that would promote and support direct consumption of solar energy in a more optimal way. The overall use case can be seen in Figure 4.

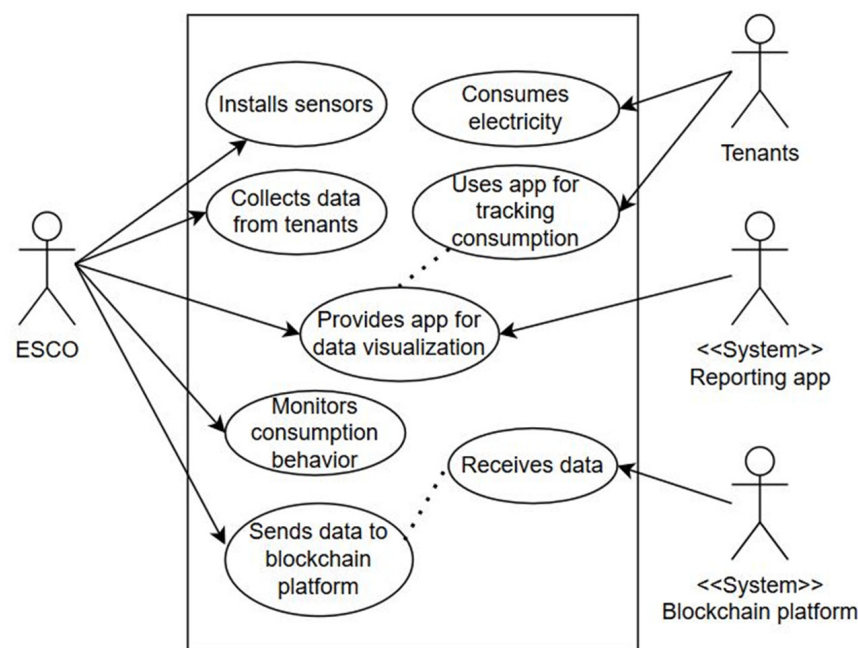


Figure 4. Use case diagram with overview of the Berlin use case (authors' illustration).

4.1. MRV Framework in the Berlin Use Case

The MRV framework implemented in this use case provides a structured approach to monitor, document and validate energy efficiency improvements and energy savings, while fostering tenant engagement and encouraging sustainable behavior.

Measurement: Modern digital electric meters are deployed in the building complex to collect metering data on solar energy production and consumption patterns. These

metering systems gather information not only from PV systems, but also from charging stations of EVs as well as residential units. Data could be collected with high resolution (e.g., every minute). This enables comprehensive and real-time tracking of energy production and energy consumption across multiple facilities (e.g., household, PV and EV) on the site, which allows one to see the whole picture of energy production and consumption. Later on, the collected data are compared with baseline measurements; this is performed in order to reflect the delta between the building's previous energy consumption and the current consumption, so that the effects of optimization measures can be assessed. It should be noted that a longer period of data collection is required in order to calculate the optimization of the behavior changes of tenants. Therefore, measurements must be taken during both periods of normal and influenced behavior, which is achieved with help of mobile app/tokens-based incentivization. Additionally, due to seasonal variations in energy production (e.g., winter and summer) and consumption, both periods should be at least 1 year. Therefore, baseline measurements could be calculated based on normal behavior over a period of one year.

Reporting: The app serves as the primary reporting tool, offering tenants real-time visibility into their energy consumption and the solar energy production on the rooftops. This level of transparency empowers tenants to monitor their energy usage and make informed decisions to align their consumption with periods of peak solar production. Additionally, the app simplifies data collection and processing for project stakeholders, enabling more efficient management and evaluation of the project's progress. While future feedback mechanisms are planned, such as email-based reporting, the app already plays a crucial role in fostering tenant engagement and transparency.

Verification: Reliability of the data collected during the measurement phase is achieved through the integration of blockchain technology for calculations based on the data KPIs. The blockchain technology acts as a secure mechanism for validating energy data. Data entries are encrypted and undergo repeated calculations to verify their accuracy. Only data that meet strict consistency criteria are processed further and allowed to be stored in the blockchain platform. This approach minimizes the risk of data errors or tampering, ensuring that stakeholders can rely on the accuracy of the energy data for decision-making and reporting purposes. Figure 5 depicts the calculated PV quotas, which are based on one year of measurements from a single building (from November 2024 to October 2025).

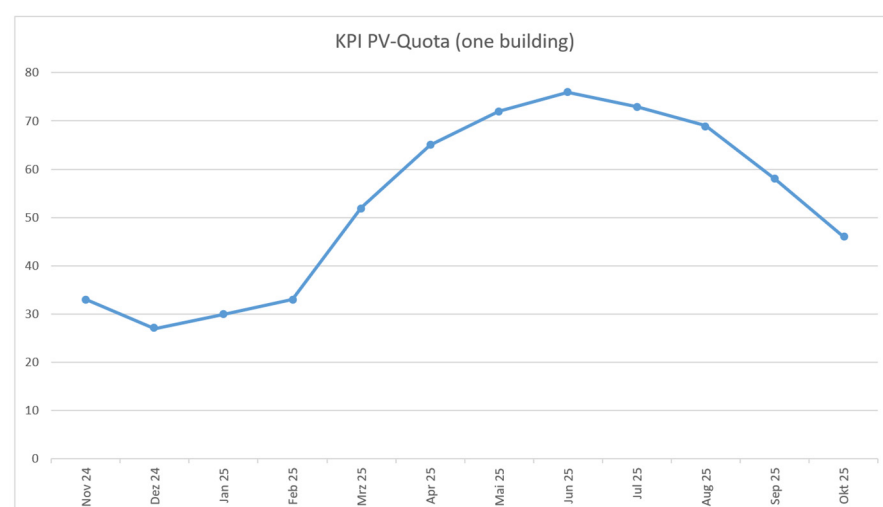


Figure 5. Demonstrates calculated PV quotas, which are calculated based on measurements of a single building over a one-year period (from November 2024 to October 2025). The PV quota increases in summer and decreases in winter.

Payment: The use case entails an additional reward element. This component introduces a motivational element designed to encourage tenants to adopt energy-efficient behaviors. The current approach uses a token-based reward system, wherein tenants (clustered by buildings) who achieve an increase in the efficiency of their roof top PV plant capacity utilization of at least 5 percent receive symbolic tokens as recognition for their efforts. In addition, the saving of energy in the tenants' households of at least 10 percent is rewarded with tokens. The tokens are generated based on the execution of a smart contract. To determine potential behavioral changes, data collected over a one-year period will be compared to a baseline from a period prior to the deployment of the measuring devices and the app. This will later be integrated into the process, allowing behavioral changes to be valued via tokens. These steps are currently underway.

These tokens serve as an incentive to align personal behavior with the sustainability goals of the project, fostering a sense of achievement and participation. Although the reward system does not yet include direct financial incentives, it seeks to determine whether symbolic rewards can drive behavioral change. Looking ahead, the MRV framework sets the stage for more advanced mechanisms, such as two-tariff models, dynamic electricity tariffs and Pay-for-Performance (P4P) schemes, which could further align individual financial incentives with broader energy efficiency objectives. As an example, for the KPI calculations, the calculation of the PV-quota is demonstrated in the following formula in Equation (1).

$$KPI\ quota, day = \frac{\sum_{i=15\ min}^{day} Q_{Production,i}}{\sum_{i=15\ min}^{day} Q_{Demand,i}} \quad (1)$$

Equation (1) is an example of calculation of KPI quota with the boundary conditions. The purpose of the equation is to illustrate how the KPI would be typically calculated.

Data sovereignty: In the context of the Berlin use case, data sovereignty is part of the MRV framework by design, ensuring compliance with GDPR and addressing the unique challenges associated with managing sensitive energy data from tenants. The use case involves the deployment of digital meters and sensors to collect real-time data on solar energy production and consumption. These data, crucial for evaluating and optimizing energy efficiency, must remain under the control of tenants and stakeholders, adhering strictly to EU regulations. Data sovereignty ensures that tenants retain ownership of their energy data, determining how it is collected, stored and used while protecting privacy and security. Thus, before KPIs based on the collected data are stored in the blockchain, the sensitive information is encrypted using a special hash algorithm. Only data that are important for verification are stored in a blockchain. For instance, for each KPI (e.g., PV-Quota), a new block on a blockchain must be calculated. To calculate a block, a special smart workflow must be initiated. In this particular case, 'a smart workflow' is a process that communicates with the blockchain and calculates the Merkle tree hash using KPI calculations as input. This smart workflow runs on a local server and retrieves the KPI calculation via HTTP from a software component designed to calculate various KPIs (e.g., PV-Quota) using measurements gathered from tenants. In order to complete the smart workflow, three nodes running the same smart flow must be started and a leader selected from among them. These running smart flows must then reach a consensus so that a new block can be stored on the blockchain. Calculating the KPIs for a single month of data takes around one minute (the data must be pulled over HTTP). The smart workflow takes between 17 and 20 min to find a consensus. The entire process takes a little over 20 min. Verification processes within the use case leverage blockchain technology, aligning with data sovereignty principles by securing data integrity through decentralized,

transparent mechanisms. Blockchain ensures that collected data are immutable and tamper-proof, which is critical for building trust among stakeholders. However, the integration of blockchain also presents specific challenges, such as anonymizing data to comply with GDPR requirements for erasure and privacy while maintaining its usability within the MRV framework. Careful planning and technical implementation are required to balance these regulatory demands with the functional needs of the use case.

The reporting component, managed through the app, exemplifies the operationalization of data sovereignty within the use case. The app provides tenants with real-time access to their own electricity consumption and the PV production on their rooftops, while ensuring that data sharing remains within the legal frameworks governing its collection. The app's design emphasizes transparency and controlled access, reinforcing tenant trust and engagement by aligning with data sovereignty principles.

In the payment dimension, symbolic token-based rewards incentivize tenants to adopt energy-efficient behaviors. Data sovereignty ensures that personal data used to calculate and distribute rewards is securely managed, with tenants retaining control over how their data are utilized. This approach reinforces the ethical and trust-based foundation of the MRV framework, while supporting the broader sustainability goals of the use case.

4.2. SGAM Visualization of the Berlin Use Case

To determine which design options are suitable for the MRV framework, the IEC 62559-2 Use Case methodology is used. As seen in pink in Figure 6, the business layer explicitly incorporates the P4P schemes and reflects the primary objectives of the use case, including the KPIs “Solar energy optimization” and “Reduction in energy costs”. By situating these elements on the business layer, the model highlights how strategic goals and regulatory requirements are operationalized within business processes and interactions between actors in the smart grid environment. On the functional interoperability layer, here in on the right side of Figure 6 (in blue), the services provided by the MRV system and buildings are shown, such as storing energy information and calculating KPIs and authenticating identities on the market, installing metering devices, putting the app into action and performing KPI calculations on the enterprise level, as well as metering on the station level and consuming/producing on the process level.

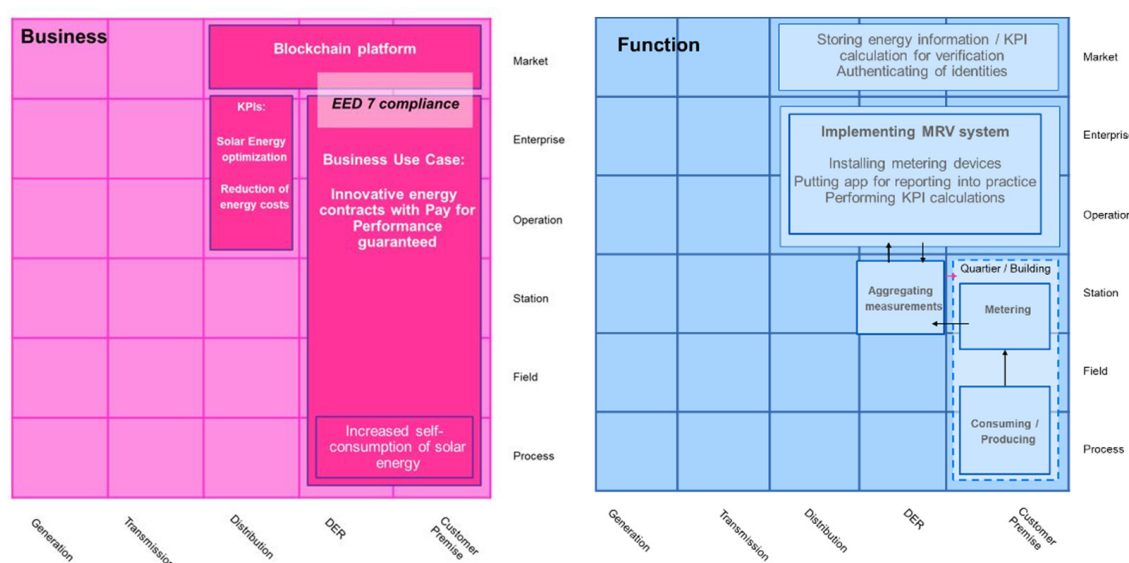


Figure 6. Business and function layer of SGAM mapped to the Berlin use case and MRV (authors' representation).

On the information interoperability layer in Figure 7, a variety of standards are applied to ensure consistent and accurate data exchange across the system. For enterprise and operational functions, standards such as IEC 62746, IEC 61968 and IEC 61400-25 are employed. For station-level communication, IEC 61400-25 and IEC 61850 are implemented, while process-level interactions are fully supported by IEC 61850. Additionally, standards related to emerging technologies, such as ISO/TC 307 for blockchain and distributed ledger technologies (DLTs), are incorporated to facilitate secure and verifiable reporting. The communication layer of the SGAM illustrates the various protocols and APIs that enable interoperability between different system components. At the market level, TCP/IP is used to facilitate reliable data exchange. Within the enterprise and station layers, REST APIs are employed to support standardized, web-based communication. Wide Area Network (WAN) connections are implemented at the station level to ensure connectivity over large distances, while the CLS protocol is utilized at both station and field levels to manage control and signaling functions. For process-level interactions, a combination of communication technologies—including Broadband over Power Lines (BPL), Ethernet (LAN), and Long Range (LoRa)—is applied to ensure robust and flexible data transmission across diverse operational devices and field equipment. By mapping these protocols and interfaces onto the communication layer, the SGAM provides a clear overview of how data flow across all levels of the smart grid, supporting both operational efficiency and system interoperability.

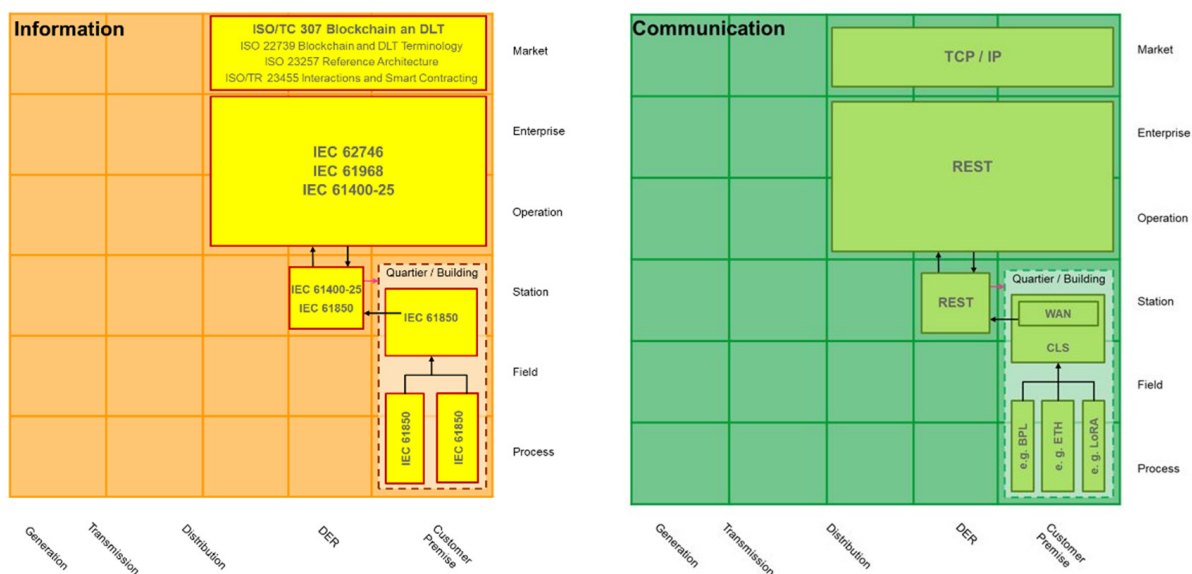


Figure 7. Information and communication layer of SGAM (authors' representation).

Finally, the component interoperability layer in Figure 8 displays all actors and systems involved in the use case. This includes the MRV system, an aggregator, building owners and customers, with the latter directly linked to the smart meters, PV systems, and EV charging stations. MRV spans all interoperability layers of the SGAM, from the business layer down to the process layer, ensuring that measurement, reporting, and verification are consistently integrated throughout the system. Its implementation covers all levels of the smart grid, from market operations to enterprise, station, and field processes, enabling seamless data flow and traceability across actors and devices. The arrows show that data from the digital meter goes to the MRV dashboard and also flows back within the neighborhoods/buildings to tenants, for example.

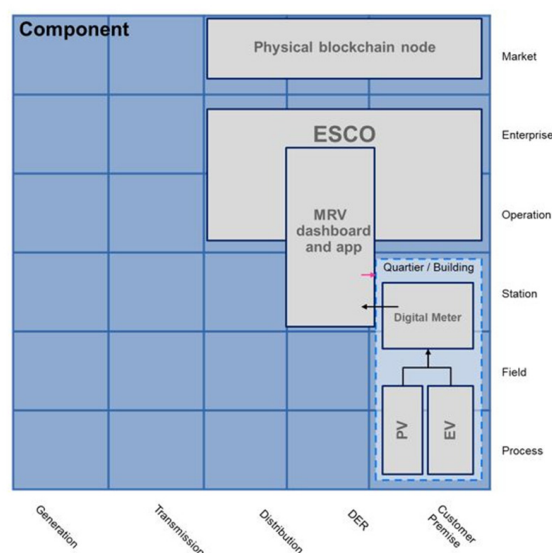


Figure 8. Component layer (authors' representation).

The final SGAM visualization in Figure 9 illustrates the complete use case across all interoperability layers, namely business, function, information, communication, and component, providing a comprehensive representation of the system architecture and its cross-layer interactions.

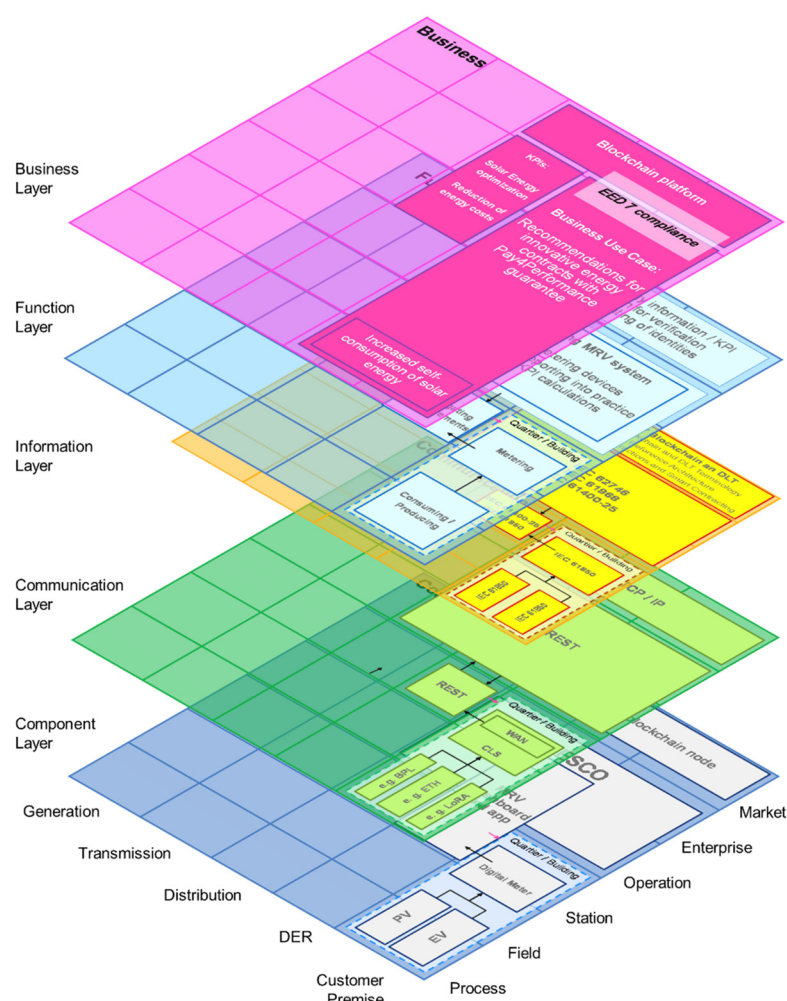


Figure 9. SGAM representation.

5. Discussion

This study demonstrates that the MRV concept introduced under EED 8 can be translated into an actionable organizational framework for smart buildings by operationalizing its core principles, namely interoperability and data sovereignty. This section discusses how the MRV concept was implemented in the use case in regard to the design options stated in Section 3, with particular emphasis on the alternative approaches that emerged from this implementation.

5.1. Implementing an MRV Framework with a Mobile App for Data Reporting and Blockchain for Verification

Implementing a robust MRV framework is essential for ensuring transparency, accuracy and trust in demonstrating energy efficiency in smart buildings. In the Berlin use case, an MRV framework has been implemented using digital meters for measurement (M), an app that calculates key performance indicators (KPIs) for reporting (R) and blockchain technology for the verification (V). The result was an efficient, transparent and trustworthy framework that enhances data integrity, while enabling timely decision making and accountability across stakeholders in the use case. EED 8 compliance, data sovereignty and interoperability have therefore been included in the considerations of the use case.

Looking closer at *measurement (M)*, tenants must have access to accurate and up-to-date energy data, either in real time or at regular intervals. When digital meters are installed, the directive mandates that they support secure, reliable and user-friendly data transmission. These requirements are fulfilled by the app in the use case, which enables tenants to access and view their consumption data in a transparent manner. As the data collection period spanned only one year, it was not possible to measure or reliably estimate substantive behavioral changes among tenants based on these data. Nevertheless, a dedicated methodological framework has been developed that is expected to enable the measurement and estimation of such behavioral shifts over a longer observation period. One approach is to establish a power consumption baseline, which will be compared to new KPIs calculated using the newly gathered data. This will be achieved through a combination of smart contract processes (e.g., producing tokens based on behavioral changes) and gamification processes (e.g., incentivizing behavior).

According to EED 8 demands for *reporting (R)*, sufficient and detailed data needs to be provided to analyze consumption patterns and encourage efficiency measures. The data transmitted from the digital meter to the app in the use case exhibit a level of granularity sufficient to enable tenants to identify their consumption patterns. This level of detail provides the necessary information for tenants to make informed decisions and adopt more energy-efficient behaviors, such as scheduling the charging of electric vehicles during specific time periods. EED 8 and GDPR both consider energy data as personal data due to the link to a specific user. In the use case, informed consent for data processing was obtained. Similarly, the app operated by the ESCO and used by the tenants implements stringent measures to ensure data security during data processing. Data transmission is encrypted and protected from unauthorized access. Although the app is installed on the user's device, data from the supported devices is transmitted to the ESCO via the cloud, enabling the ESCO to monitor energy consumption at a detailed level.

Focusing on the key requirements outlined in Section 3, such as *data sovereignty*, it becomes clear that cloud computing via the app is subject to the regulations and laws of the country in which the cloud platform is located and where the data are stored [40]. In this use case, the app is developed by a German software company; therefore, the data would fall under the jurisdiction of the cloud providers, which could be considered as critical for the *privacy* compliance of MRV data. Specifically, MRV data encompass personal data,

such as the metering or EV data of individual tenants. To ensure the *secure* transmission of MRV data, cloud service providers must comply with the GDPR. Nevertheless, even with restricted access, a cloud-based system is inherently more susceptible to cyberattacks compared to alternatives, such as data spaces or blockchain architectures. Consequently, the implementation of robust security mechanisms is essential in the use case, particularly when personal data are processed and reported through cloud-based technologies. However, a degree of interdependence persists between the ESCO and the app provider, which developed the app on behalf of the ESCO. Similarly, tenants must be able to trust both the ESCO and the app provider to ensure the security of their data.

For *verification*, blockchain technology is used. By decentralizing and providing control over MRV data through digital identities, blockchain can generally adhere to aspects of data sovereignty. Owing to its decentralized nature, data sovereignty rests with individuals who possess access, rather being centralized. Regarding *privacy*, blockchain technology offers a transparent way to store and share data, as only permitted users can access the data. All in all, the energy data recorded on a blockchain is transparent and auditable by all blockchain users. However, in the use case, only aggregated KPI calculations are stored on the blockchain that are needed for the calculation of the tokens. To this end, the collected data was aggregated, used to calculate KPIs, and anonymized before being transferred to the blockchain. An ESCO can access and verify the energy data once they have been stored in the blockchain, while the tenants are disconnected from the blockchain via anonymization and aggregation steps. As only aggregated KPI calculations with no personal information are stored on the blockchain, there is no conflict with personal data on the blockchain. The integration of blockchain technology emerged as a particular technical challenge in the Berlin use case. The process required the support of specialized blockchain experts to be successful. Furthermore, even after all the data were gathered and the data integration pipelines were in place, integrating the blockchain could have been a time-consuming step. The insights gained from this Berlin use case are especially pertinent for teams lacking prior experience with blockchain technology and should inform the planning and design of comparable projects.

Having a look at *data sovereignty*, it is necessary to critically consider the security properties of the blockchain. Regarding the *security* aspect, the blockchain technology offers a secure way to store and share data, as it is based on a decentralized database that is shared by many users. This minimizes the risk of data loss or manipulation. Hence, the blockchain ensures tamper-proof records. The distributed nodes verify all transactions, while reducing reliance on a central authority. This enhances security against single points of failure. Additionally, blockchain's decentralized and distributed ledger system empowers actors with greater control over their data, ensuring transparency and consistency. From this viewpoint, blockchain technology generally offers *trust* through decentralization, transparency and immutability. From an ethical point of view, the MRV data within a blockchain can only be accessed by authorized persons with a private key. This minimizes the risk of data loss or manipulation.

Integrating blockchain technologies into existing energy infrastructure poses significant challenges related to *interoperability*, thereby underscoring the necessity for interoperable and harmonized standards. A prominent example concerns the MRV data, which, once stored on the blockchain, are inherently difficult to delete or modify. This characteristic conflicts with the principles of the GDPR, particularly with the right to data erasure and the requirement for controllability of personal data. Overall, it can be said that blockchain has a certain degree of market maturity and is already widely developed in various domains. Although no large-scale or standardized applications of blockchain for MRV data currently exist, the technology nonetheless offers substantial potential for secure and transparent

data management. Given that blockchain concepts are well established and extensively tested, their practical implementation has progressed, and they are already being applied to energy data management systems.

The study also showed that implementing a fully integrated and sufficient MRV concept is challenging due to a number of reasons. As was already made clear, the use of different technologies for the management of data has various effects on the use case architecture and therefore on the successful development of an MRV framework. Another critical element that warrants attention is the synergistic relationships within MRV frameworks, the absence of which makes an implemented MRV framework inoperable. Consequently, these three constituents are interconnected and must be considered altogether as complementary aspects, rather than in segregation. Integrating MRV frameworks with real-time energy monitoring enables organizations to shift from periodic reporting toward ongoing performance optimization, thereby enhancing transparency and accountability in energy efficiency measures. Moreover, aligning MRV responsibilities with organizational governance structures and decision-making processes appears critical for translating regulatory requirements into actionable energy-saving initiatives. This development positions MRV not only as a compliance mechanism but as a strategic management tool that supports continuous improvement and long-term energy efficiency gains in smart buildings.

5.2. Alternative Approaches to MRV with Data Spaces

Alternative approaches to the data reporting and verification parts of the MRV framework are presented in methodologies developed under the European *data space* initiative. The Data Governance Act (DGA) is a European regulation that seeks to establish a framework for the development of European data spaces. The DGA has important implications for MRV frameworks. By establishing European data spaces, the DGA promotes greater trust and standardization among data providers, which can enhance the reliability and comparability of MRV data. However, participation in data spaces is limited to actors who meet specific governance and regulatory requirements, potentially restricting the pool of data sources. MRV frameworks must therefore adapt to these compliance obligations when integrating data from such spaces. Overall, data spaces offer opportunities to improve MRV through more interoperable, verifiable, and high-quality data, while also introducing constraints related to access and regulation. However, the existing literature provides limited insight into the operational functioning of data spaces and the conditions under which they can be effectively utilized. In particular, stakeholders are required to comply with a range of regulatory and governance requirements to participate in a data space [42].

Achieving *interoperability, data sovereignty, privacy and security* is one of the main aims for data spaces, as they follow the principles of transparency and open standards. For example, interoperability is one of the main objectives for a Gaia-X-conformant data space and therefore equally necessary for the management of MRV data. While data sovereignty is generally ensured in data spaces, the market maturity of data spaces is rather low today, as only a few data spaces have actually been implemented (e.g. in the automotive sector). A fully operational data space within the energy sector has not yet been implemented.

6. Conclusions and Outlook

Developing an EED 8-compliant, interoperable, and sovereign MRV framework remains a challenging yet essential task for supporting EU regulations and guidelines on future EE measures in smart buildings. This study highlights the existing uncertainties and gaps in designing a comprehensive MRV framework applicable to EEM in this context. To address this gap, this study presents a real-world use case that demonstrates the feasibility of a framework capable of integrating these requirements. The findings provide a founda-

tion for future research and practical implementation of MRV systems in smart building energy management.

Accurate data measurement (M) within buildings is a critical prerequisite for the effective implementation of MRV systems. Although deployment has been slow to date, its adoption is expected to be further accelerated by the provisions of §14a EnWG, which confer additional relevance to these activities. Data reporting (R) from the smart building via the app is straightforward and facilitates the transmission of large volumes of data, including real-time streams. However, such reporting mechanisms require robust security measures to ensure data protection and maintain data sovereignty. Likewise, control over the data resides with the app provider, creating a dependency between an ESCO and the app provider.

With regard to the verification (V) of data, the blockchain-based design option represents a market-ready, sovereign and interoperable solution in smart buildings. However, significant limitations arise in the regulatory context, as blockchain-based data structures do not allow for the straightforward deletion of data or subsequent modification of the chain due to their inherent immutability. However, as only aggregated data derived from the KPI calculations are transferred to the blockchain in the Berlin use case, no personal data are stored on the ledger. To obtain further empirical insights and validate the applicability of the developed MRV framework within the use case, the framework can be tested in other use cases and over longer periods. The results of a long-term study of the MRV framework implementation can be published in future research.

At the same time, data spaces have proven to be an interesting alternative approach for the implementation of an MRV framework. Data spaces play an increasingly important role today as a secure, interoperable and sovereign data ecosystem. However, there are currently no existing approaches for an MRV framework using a data space. Research and practical approaches to implementation could close this research gap. Consequently, even if the aspects of data sovereignty are covered by data spaces, there is still too little market maturity to be able to present MRV data in such a data ecosystem. Nevertheless, data spaces appear to be a particularly future-oriented decentralized data concept, especially for MRV data.

To conclude, the study showed that a comprehensive MRV framework can enable the implementation of EEM as well as the demonstration of compliance with national or international commitments and standards. The development of an MRV framework can lead to greater transparency and accountability of EE actions and is necessary to provide feedback and learning for improving performance and impact of EE.

Author Contributions: Writing—original draft preparation: J.K.; A.B.-P., V.D., F.T.; Writing—review and editing: J.A. All authors have read and agreed to the published version of the manuscript.

Funding: This paper has received funding from the European Union under grant agreement No.101080029 as part of the InEEsS (Innovative Energy Efficiency Services) project under ID101077033. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

Data Availability Statement: The datasets presented in this article are not readily available due to data restriction regulations. Requests to access the datasets should be directed to Berliner Energie Agentur.

Conflicts of Interest: Authors Julia Petra Köhlke, Viktor Dmitriyev and Jad Asswad were employed by the research institute OFFIS e.V. Institute for Information Technology. Authors Anna Brüning-Pfeiffer and Franziska Tucci were employed by the company Berliner Energieagentur GmbH. The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

API	Application Programming Interface
APMs	Alternative Policy Measures
CLSs	Controllable Local Systems
COP 13	The Bali Action Plan of Conference of Parties 13
DSO	distribution system operator
EC	European Commission
EE	energy efficiency
EED	energy efficiency directive
EEM	energy efficiency measures
EEOS	Energy Efficiency Obligation Schemes
ESCO	energy service company
ETS	Emissions Trading System
EU	European Union
EV	electric vehicle
GDPR	General Data Protection Regulation
IPMVP	The International Performance Measurement and Verification Protocol
KPIs	key performance indicators
LAN	Local Area Network
LoRa	Low Range
M&V	Measurement and Verification
MRV	Measurement, Reporting and Verification
NAMA	Nationally Appropriate Mitigation Action
NEEAP	National Energy Efficiency Action Plan
P4P	Pay-for-Performance
PV	Photovoltaics
REST	Representational State Transfer
SGAM	Smart Grid Architecture Model
WAN	Wide Area Network

References

1. Von Malmborg, F. First and last always: Politics of the ‘energy efficiency first’ principle in EU energy and climate policy. *Energy Res. Soc. Sci.* **2023**, *101*, 103126. [[CrossRef](#)]
2. Li, H.; Johra, H.; Pereira, F.d.A.; Hong, T.; Le Dréau, J.; Maturo, A.; Wei, M.; Liu, Y.; Saberi-Derakhthenjani, A.; Nagy, Z.; et al. Data-driven key performance indicators and datasets for building energy flexibility: A review and perspectives. *Appl. Energy* **2023**, *343*, 121217. [[CrossRef](#)]
3. Kristombu Baduge, S.; Thilakarathna, S.; Shalitha Perera, J.; Arashpour, M.; Sharafi, P.; Teodosio, B.; Shringi, A.; Mendis, P. Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Autom. Constr.* **2022**, *141*, 104440. [[CrossRef](#)]
4. Lamnatou, C.; Chemisana, D.; Cristofari, C. Smart grids and smart technologies in relation to photovoltaics, storage systems, buildings and the environment. *Renew. Energy* **2022**, *185*, 1376–1391. [[CrossRef](#)]
5. Bertoldi, P.; Mosconi, R. Do energy efficiency policies save energy? A new approach based on energy policy indicators (in the EU member states). *Energy Policy* **2020**, *139*, 111320. [[CrossRef](#)]
6. Schmidt, C.; Li, W.; Thiede, S.; Kornfeld, B.; Kara, S.; Herrmann, C. Implementing key performance indicators for energy efficiency in manufacturing. *Procedia CIRP* **2016**, *57*, 758–763. [[CrossRef](#)]
7. EVO. *International Performance Measurement and Verification Protocol (IPMVP)—Core Concepts*; Efficiency Valuation Organization: Washington, DC, USA, 2022.
8. Paustian, S.; Köhlke, J.; Mattes, J.; Lehnhoff, S. The (still unexplored) social side of smart grid development. In *The e-Energy ‘22: The Thirteenth ACM International Conference on Future Energy Systems*, Online, 28 June–1 July 2022; Association for Computing Machinery: New York, NY, USA, 2022.
9. Pérez, S.; Hernández-Ramos, J.L.; Matheu-García, S.N.; Rotondi, D.; Straniero, L.; Pedone, D. A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios. *IEEE Access* **2018**, *6*, 11738–11750. [[CrossRef](#)]

10. Gholamzadehmir, M.; Del Pero, C.; Buffa, S.; Fedrizzi, R.; Aste, N. Adaptive-predictive control strategy for HVAC systems in smart buildings—A review. *Sustain. Cities Soc.* **2020**, *63*, 102480. [CrossRef]
11. Tzani, D.; Thomas, S.; Stavrakas, V.; Rosenow, J. Pioneering a performance-based future for energy efficiency: Lessons learnt from a comparative review analysis of pay-for-performance programmes. *Renew. Sustain. Energy Rev.* **2022**, *158*, 112162. [CrossRef]
12. Singh, N.; Finnegan, J.; Levin, K. *MRV 101: Understanding Measurement, Reporting, and Verification of Climate Change Mitigation*; Working Paper; World Resources Institute: Washington, DC, USA, 2016; Available online: <http://www.wri.org/mrv101> (accessed on 13 January 2026).
13. Zusan, E. Buildings: A comparative analysis of MRV methodologies. In *Measurement, Reporting and Verification (MRV) for Low Carbon Development: Learning from Experience in Asia*; Institute for Global Environmental Strategies: Tokyo, Japan, 2023.
14. Fraunhofer Institute for Software and Systems Engineering ISST. *Handbook on Measurement, Reporting and Verification*; United Nations Framework Convention on Climate Change: Bonn, Germany, 2014.
15. Fawcett, T.; Rosenow, J.; Bertoldi, P. Energy efficiency obligation schemes: Their future in the EU. *Energy Effic.* **2019**, *12*, 57–71. [CrossRef]
16. Efficiency Valuation Organization. *International Energy Efficiency Financing Protocol (IEEFP)*; Efficiency Valuation Organization: Washington, DC, USA, 2021; Available online: https://evo-world.org/images/denisdocuments/IEEFP_TOC_2021_2.pdf (accessed on 13 January 2026).
17. Böck, M.; Ploiner, A. Setting Up an MRV System—Step-by-Step Guidance. 2021. Available online: https://energysavingpolicies.eu/wp-content/uploads/2023/05/MRVGuide_AEA_Final20211108.pdf (accessed on 13 January 2026).
18. Ensmov. Cost Effectiveness for Monitoring, Reporting and Verification (Article 7 EED). 2020. Available online: https://energysavingpolicies.eu/wp-content/uploads/2023/05/Cost-effectiveness-for-Monitoring-Reporting-and-Verification-Art-7-EED_final.pdf (accessed on 13 January 2026).
19. Europe Economics. Evaluation of Fiscal Measures in the National Policies and Methodologies to Implement Article 7 of the Energy Efficiency Directive. 2016. Available online: <https://circabc.europa.eu/ui/group/8f5f9424-a7ef-4dbf-b914-1af1d12ff5d2/library/e828e47e-ab09-4fc0-ad28-897673dd686a/details> (accessed on 13 January 2026).
20. European Commission. *The Energy Efficiency Directive—Article 8 EED*; European Commission: Brussels, Belgium, 2023; Available online: https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive_en (accessed on 13 January 2026).
21. Goorden, L.; Bourgois, J.; Wuyts, B.; Coolen, J. Guidelines for the Design of P4P Schemes. 2022. Available online: <https://zenodo.org/records/6367999> (accessed on 13 January 2026).
22. Papadelis, S. Methods for the Dynamic Measurement and Verification of Energy Savings. 2021. Available online: <https://zenodo.org/records/4695123> (accessed on 13 January 2026).
23. Federal Energy Management Program (FEMP). *M&V Guidelines: Measurement and Verification for Performance-Based Contracts*, Version 4.0. U.S. Department of Energy: Washington, DC, USA, 2015. Available online: https://www.energy.gov/sites/prod/files/2016/01/f28/mv_guide_4_0.pdf (accessed on 13 January 2026).
24. Dove, E.S. The EU General Data Protection Regulation: Implications for international scientific research in the digital era. *J. Law Med. Ethics* **2018**, *46*, 1013–1030. [CrossRef]
25. Hummel, P.; Braun, M.; Augsberg, S.; Dabrock, P. Sovereignty and data sharing. *ITU J. ICT Discov.* **2018**, *2*, 984–986. Available online: <https://www.itu.int/en/journal/002/Documents/ITU2018-11.pdf> (accessed on 13 January 2026).
26. Hellmeier, M.; Pampus, J.; Qarawlus, H.; Howar, F. Implementing data sovereignty: Requirements & challenges from practice. In *18th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2023*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1–9.
27. Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P. Data sovereignty: A review. *Big Data Soc.* **2021**, *8*. [CrossRef]
28. Jarke, M.; Otto, B.; Ram, S. Data sovereignty and data space economy. *Bus. Inf. Syst. Eng.* **2019**, *61*, 549–550. [CrossRef]
29. Annadurai, C.; Sikora, A.; Welte, D. Distributed Authentication using Self Sovereign Identities. In *2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI), Sana'a, Yemen, 25–26 November 2024*; IEEE: New York, NY, USA, 2024; pp. 1–8. [CrossRef]
30. Singi, K.; Gon Choudhury, S.; Kaulgud, V.; Chandra Bose, R.P.; Jagadeeshad Podder, S.; Burden, A.P. Data Sovereignty Governance Framework. In *ICSE '20: 42nd International Conference on Software Engineering, Seoul, Republic of Korea, 27 June 2020–19 July 2020*; Association for Computing Machinery: New York, NY, USA, 2020.
31. Floridi, L.; Taddeo, M. What is data ethics? *Philos. Trans. R. Soc. A* **2016**, *374*, 2083. [CrossRef]
32. Asswad, J.; Marx Gómez, J. Data ownership: A survey. *Information* **2021**, *12*, 465. [CrossRef]
33. Lansing, J.; Sunyaev, A. Trust in cloud computing: Conceptual typology and trust-building antecedents. *Data Base Adv. Inf. Syst.* **2016**, *47*, 58–96. [CrossRef]
34. Bertino, E. The quest for data transparency. *IEEE Secur. Priv.* **2020**, *18*, 67–68. [CrossRef]

35. Geisler, S.; Vidal, M.-E.; Cappiello, C.; Loscio, B.; Gal, A.; Jarke, M.; Lenzerini, M.; Missier, P.; Otto, B.; Paja, E.; et al. Knowledge-driven data ecosystems toward data transparency. *ACM J. Data Inf. Qual. JDIQ* **2022**, *14*, 1–12. [[CrossRef](#)]
36. Fraunhofer Institute for Software and Systems Engineering ISST. Data sovereignty and data space economy. *Bus. Inf. Syst. Eng.* **2019**, *61*, 549–550. [[CrossRef](#)]
37. Gottschalk, M.; Uslar, M.; Delfs, C. *The Use Case and Smart Grid Architecture Model Approach*; Springer: Cham, Switzerland, 2017.
38. IEC 62559-1; Use Case Methodology–Part 1: Definition of the Use Case Template. International Electrotechnical Commission: Geneva, Switzerland, 2019.
39. Thyagaturu, A.; Nguyen, G.; Rimal, B.; Reisslein, M. Ubi-Flex-Cloud: Ubiquitous flexible cloud computing: Status quo and research imperative. *Appl. Comput. Inform.* **2022**. *Epub ahead of printing*. [[CrossRef](#)]
40. Damour, F. The first blockchain: Bitcoin, entropy, religion. *J. Relig. Sci.* **2022**, *59*, 280–301. [[CrossRef](#)]
41. Hoppe, C.; Schmelzer, R.; Möller, R.; Schoorman, T. Data spaces as enablers for sustainability. In *Nachhaltige Wertschöpfungssysteme (NaWerSys) 2023, Berlin, Germany, 29 September 2023*; Gesellschaft für Informatik e.V.: Bonn, Germany, 2023.
42. Asswad, J.; Dmitriyev, V.; Elizondo Guerrero, M.E.; Theesen, C.; Köhlke, J. Requirements Engineering Approach for Data Ownership Concepts. *Electronics* **2025**, *14*, 1288. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.