

ARTÍCULOS DE DERECHO DE LA UNIÓN EUROPEA**BETWEEN ENERGY
EFFICIENCY AND PRIVACY:
SMART DATA UNDER EU LAW***Alejandra Ochoa Jiménez (4º GDL)***Abstract**

The European energy transition has made smart meters a central infrastructure for integrating renewable energy, managing electricity demand and advancing decarbonisation; yet these devices do more than optimize the electricity system, as they generate continuous and highly granular data flows that can reveal patterns of behaviour, habits and vulnerabilities within its users. Although smart meters were introduced to benefit consumers and support the European Union's climate objectives, their deployment has created a structural tension between energy and data regulation, resulting in a complex legal framework that is difficult to navigate both for citizens seeking to safeguard their privacy and for companies aiming to innovate and develop new markets in the emerging data economy. Against this background, this article explores how smart meter data is governed in practice at the intersection of EU energy legislation and data protection law, examining the challenges posed by the application of the GDPR in a multiactor electricity system and the implications of the emerging European data economy for the use and sharing of such data.

Introduction

The European energy transition has transformed smart meters from a merely technical device into a central piece of infrastructure for the digitalisation of electricity networks and the broader project of decarbonisation. These meters are now essential for integrating renewable energy, managing demand in real time and enabling more flexible and efficient electricity systems. At the same time, however, they generate continuous and highly granular consumption data that can reveal intimate details about household behaviour. What was once a simple technical measurement has become a complex flow of personal data with significant social, economic and regulatory implications. Smart meters are not only tools for market efficiency or consumer empowerment, but key enablers of the Union's decarbonisation strategy and of the large-scale electrification of society. Their data is likely to become even more important in the future for managing digital grids, improving the integration of renewables and designing new energy services. This places smart meters at a difficult intersection between energy regulation and data governance in the European Union.

There is already a substantial body of law governing both electricity markets and personal data. However, this framework was not really designed with a device like the smart meter in mind. As a result, existing rules, although robust in principle, are not always well adapted to such a highly technical, multi-actor and data-intensive energy ecosystem. The challenge is therefore not the absence of regulation, but rather its fragmentation and lack of sectoral concretisation, which creates legal uncertainty both for consumers seeking to protect their privacy and for companies attempting to innovate in the emerging European data economy.

This article examines how smart meter data is currently governed under EU law, focusing on the interaction between energy legislation and data protection rules. Rather than proposing a comprehensive reform, it offers a legal mapping of the main frameworks that apply or may apply to smart metering and highlights some of the tensions and inconsistencies that arise in practice. Particular attention is paid to questions such as the nature of smart meter data as personal data, the difficulty of identifying responsible actors in a multi-layered electricity system, and the implications of treating energy data as both a protected personal right and a potential economic resource.

Smart meters play a dual role: they are devices that produce highly sensitive personal data, but they are also strategic infrastructure for climate action and for the European economy. This makes it particularly urgent to reflect on whether the current legal architecture is sufficiently coherent and workable in practice. A clearer and more sectorally adapted framework would be better placed to protect individuals' privacy while also unlocking the full potential of smart meter data for innovation, economic growth and the collective goal of reducing greenhouse gas emissions.

I. Smart Metering at the Intersection of Energy Regulation and Data Protection

1.1 Smart Meters

In order to have electricity, consumers whether residential, industrial or commercial, contract with an electricity supplier company which sells them the resources they need. But these companies are often not the direct producers of electricity, depending on the circumstances of each Member State of the European Union. On the grid there are various phases that incorporate different actors (producers, transmitters, distributors and ultimately commercial suppliers), all of which need to coordinate and be able to accurately predict the amount of energy that needs to be supplied and the amount that will be consumed. For the electricity sector to work properly, avoiding grid failures and provide for revenues, electricity production and consumption always need to be balanced (Van Aubel, 2023). Traditionally, electricity suppliers determined the amount that was to be consumed based on predictions deriving from manually reading analog meters, and they would buy the electricity from the producers at wholesale markets, then transmitter and distributor operators make sure to maintain the supply and demand sides balanced,

and afterwards a settlement is reached based on how much electricity was actually consumed in the agreed period. Again the electricity supplying companies used analogue meters to determine this amount and bill their clients accordingly, but when needed to be read manually, most of this business was based on predictions.

The fast paced introduction of renewable energy sources to the grid added an additional layer of difficulty, because the generation of solar and wind energy is characterized by being hard to predict as it entirely depends on weather conditions. Additionally, actors who had traditionally acted as consumers can become producers of energy, for example a building feeding its surplus energy obtained from solar panels into the grid. It can be observed there's a lot more uncertainty when it comes to accurately predicting how much electricity will be consumed.

Coupled to other issues such as grid capacity, there was an immediate need to upgrade the grid system and the solution was the digitalization of the grids, which included as a the most visible change for consumers, the introduction of smart meters. Meters are the point where the electricity grid and the building or unit of the consumer meet. Smart meters as defined by Directive (EU) 2019/944 are electronic systems which can measure the electricity fed into the grid or the electricity consumed from it, providing more information than a traditional meter, and being capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication. Therefore the most obvious distinction between a traditional meter and a smart meter is the capacity to remotely collect data of the electricity consumption and being able to transmit it (Lee & Hess, 2021). This creates an innate tension that was not self-evident before, for decades meter data consisted purely in a number that consumers would pass to their distributors or suppliers that is not privacy sensitive. However smart meters are capable of collecting data with extreme precision over very short time slots, creating concerns over privacy, which will be addressed in detail further on.

An important consideration is the number of actors that can have access to the data obtained from smart meters. While before the deployment of smart meters the communication was seemingly bilateral between the consumer and the distributor operator (or supplier directly depending on each Member States), nowadays it is more complex and it is important to understand its implications. As mentioned before, consumers contract with electricity suppliers, but suppliers most of the time, depend on the infrastructure of distributor operators, typically they are the ones in charge of the installation of smart meters and of collecting the readings. In consequence, the distributor has to transmit and communicate the data to the supplier of electricity. But other actors can also have access to the data recorded, these for instance can be independent service providers, who offer additional services using meter readings, e.g. a smartphone app to save energy (Van Aubel, 2023), or even home appliances providers. Also, it should be kept in mind that while the rollout of smart metering systems was mandated at Union level, their concrete implementation was left to Member States, which adopted differentiated technical and regulatory approaches. At the same time, EU energy law did

not establish a specific data protection regime for smart metering, but rather required compliance with the general Union data protection framework, making Regulation (EU) 2016/679 (GDPR) the common minimum standard governing the processing of smart meter data across Member States as it will be explained in the following sections.

I.II The Regulatory Origin: Emergence of the Data Protection Tension

Today the digitalization of the Union's energy systems is framed as a core element of Europe's strategic autonomy, competitiveness and environmental sustainability strategies, however when first conceived, the purpose of the development and modernization of key critical infrastructure was a different one, specially when it comes to the electricity sector. Directive 2009/72 repealed by Directive (EU) 2019/944 set up the goal of digitalizing the electricity infrastructure of the Union with an essential motive in mind: ensuring energy efficiency and empowering consumers. By doing so, it imposed an obligation on Member States to gradually incorporate smart metering systems. Although smart metering has always been closely tied to Europe's energy and climate goals, in the beginning it was more closely directed towards benefiting and empowering consumers as a first and foremost goal and it was only later that it evolved towards being fully understood as the power behind the decarbonization of our energy systems.

Having in mind the regulatory background behind the rollout of smart meters in the European Union helps to situate the emerging tension with consumers' rights, particularly with regard to privacy. If the development and deployment of smart metering systems were originally conceived as a tool to benefit consumers, this raises the question of how their fundamental rights, including data protection and privacy, were addressed in that framework. A tension which becomes even more apparent when considering that the role of smart metering has been expanded to serve broader climate and economic objectives in a way in which they were not envisioned at the core of the original regulatory rationale.

More than a decade ago, the deployment of smart meters was not envisioned having in mind the impact of the enormous amount data it would generate and collect, although data has always been inherent to smart metering, it was not seen as much of an economic asset as it currently is and data governance was not a central regulatory concern within the objectives of that framework. Today, we have come to a reality of a data driven economy, which has resulted in a regulatory lag in smart metering, since general data protection rules, designed as a broad and horizontal framework (Lee & Hess 2021), are now having to be applied to a form of data collection that is continuous, mandatory, and particularly intrusive, without having been specifically tailored to that context.

I.III Privacy and Data Protection Risks of Smart Metering

Directive (EU) 2019/944 underlined for the first time the importance of smart metering as a powerful tool for the development of an internal electricity market primarily for the benefit of consumers. Recital 52 of the Directive recalls "Engaging consumers requires

appropriate incentives and technologies such as smart metering systems. Smart metering systems empower consumers because they allow them to receive accurate and near real-time feedback on their energy consumption or generation, and to manage their consumption better, to participate in and reap benefits from demand response programmes and other services, and to lower their electricity bills. Smart metering systems also enable distribution system operators to have better visibility of their networks, and as a consequence, to reduce their operation and maintenance costs and to pass those savings on to the consumers in the form of lower distribution tariffs”. The intention of the Directive was to introduce new rights to protect and empower electricity consumers, and smart metering is the key tool that enables consumers to exercise those rights, such as the entitlement to a dynamic price contract (Peers, 2019).

However, even with all these benefits clearly directed towards consumers, smart meters represent a genuine threat to privacy. This is because the data they collect, which may at first sight appear harmless, is recorded with such a high level of granularity that it enables the creation of highly detailed profiles of electricity users. When consumption is measured at very short time intervals, it becomes possible to identify precise patterns of behaviour that reveal far more than mere electricity usage. Through disaggregation techniques, this data can expose daily routines, periods of presence or absence in the home, and even the use of specific appliances, including sensitive devices such as medical equipment or baby monitors. As a result, the level of detail that can be extracted from smart meter data may amount to a significant intrusion into individuals’ private lives, particularly when users are unaware of who has access to their data and for what purposes it is being used.

For instance, Beckel et al explain that while utilities currently rely on consumption data mainly to improve meter-to-cash processes, enable advanced tariff schemes, and provide consumers with more detailed information on their electricity use, the same data can also be analysed to infer sensitive household characteristics. Their study shows that smart meter data can be used to derive information such as a household’s socio-economic status, employment situation or number of residents with a high degree of accuracy. Importantly, these inferences were possible even when the data analysed was recorded at 30-minute intervals, rather than at the highest level of granularity, which smart meters are technically capable of reaching. This illustrates how consumption data, even in less granular forms, may support profiling practices with significant implications for data protection.

I.IV The Protection of Data collected by Smart Meters under EU law: Uniform Protection, Diverse Management

It has been established that Directive (EU) 2019/944 governs the rollout of smart metering systems, yet it does not engage directly with the privacy implications that arise from their implementation. The Directive provides, in Article 20, that the security of data communication and the protection of final consumers’ data must be ensured in compliance with relevant Union data protection and security legislation. Further

provisions on data access and management reiterate the need to guarantee a high level of cybersecurity and data protection through the application of best available techniques. Ultimately, however, the Directive externalises data protection concerns to the Union's general data protection framework. Article 23 expressly refers the processing of smart meter data to Regulation (EU) 2016/679, while leaving the concrete organisation of data management to the Member States. As a result, it is for each Member State to determine the rules governing data management and exchange, to designate the parties entitled to access smart meter data, and, consequently, to define the allocation of roles as data controllers. This leads to an asymmetrical landscape across the Union, in which data protection formally rests on Regulation (EU) 2016/679, but the distribution of responsibilities and the level of protection afforded to consumers varies depending on the national data management model adopted.

Although Directive (EU) 2019/944 provides comprehensive principles for a standardized access to metering data and data sharing across all Member States of the European Union and outlines the obligations of the market participants, its implementation has remained inconsistent with heterogeneous national practices that lead to substantial disparities in how energy data is stored, accessed, and shared (Kashyap et al, 2025). To try to limit these inconsistencies, the Commission introduced the Implementing Regulation (EU) 2023/1162 which lays down specific requirements for data interoperability aiming to bridge the divide between the different data management models of Member States. However even with these in place and with the cover of an homogeneous personal data protection framework under Regulation (EU) 2016/679, the actual enforcement of those rights deriving from both frameworks result in inconsistencies because of the different management models (Lavrijssen et al, 2022).

I.V Nature of the Data Collected by Smart Meters

Before delving deeper into how the content of Regulation (EU) 2016/679 and Europe's energy legislation interact and the tensions that arise between them, it is important to understand what is the content of the data recorded by smart meters, because this precisely determines the application of Regulation (EU) 2016/679. For the Regulation to apply according to its Article 1 to the processing of personal data of natural persons, therefore the data collected in the energy sector that relates to companies or other non-natural persons do not fit under its scope. Article 4 defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The Article 29 Working Party gave an extensive interpretation of the term "personal data" in its Opinion 4/2007. According to the party the elements of the definition shall be

understood as follows: “information” covers any type of objective or subjective information about an individual, it can have any content and does not necessarily has to be proven true, the form in which it is contained is not relevant either. As for the term “related to” the party explains that information can be considered to be related to an individual when it is about that individual. Sometimes identifying the connection can be an obvious exercise when the content of the information is directly linked to the individual regardless of the circumstances surrounding the case, but when the information concerns for instance objects it is necessary to look into the purpose of what the data is or is likely to be used for, when it is for the purpose of evaluating, treating in a certain way or influencing the status or behaviour of an individual. Finally the term related to can arise also from the element of a result, when in absence of a direct content link or purpose, the use of the information is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. The third element is “identified or identifiable” in accordance with the Party; these are separate terms; a person is identified when it can be distinguished from the members of a group, and identifiable when it has not already been identified yet, but it is possible to do so. The definition of “personal data” of the Regulation includes a set of possible identifiers which are not exhaustive and can be used directly or indirectly. Finally the fourth element “natural person” as mentioned earlier the Regulation applies exclusively to living human beings.

Based on all the foregoing concepts and its elements it can be concluded that the data from electricity smart meters falls under the definition of personal data, and is therefore likely to be subject to Regulation (EU) 2016/679. The Article 29 Working Party had arrived at such a deduction as early as in 2011, when the exhaustion and possibilities of detailed profiling were not close to the pace in which they are today, which makes evident the incidence that smart meters have in individual's privacy today. In concrete terms, smart meter data qualifies as personal data because it is intrinsically linked to an identifiable individual. Each smart meter is associated with a unique identification number that corresponds to the person responsible for the energy contract, which makes it possible to single out that consumer from others. Moreover, the continuous recording of consumption patterns enables the construction of detailed profiles of household behaviour that are later used for decision-making, notably for billing and tariff design, but could in theory be used for other purposes. Finally, the very objective of using smart meters to influence and steer consumer behaviour in the name of energy efficiency depends on the systematic collection of information about how individuals use electricity in their daily lives. For these reasons, smart meter data cannot be treated as neutral or purely technical information, but rather as personal data within the meaning of Regulation (EU) 2016/679. However for the Regulation (EU) 2016/679 to be applicable according to Article 2, the personal data has to be processed, the processing of data has an equally broad definition under the regulation which makes the Regulation apply almost at all instances where personal data is involved. When it comes to smart meters which collect and transmit data that can be characterized as personal, they clearly fit into the category of processing.

I.VI Challenges of the Application of Regulation (EU) 2016/679 (GDPR)

Having established that smart meter data constitutes personal data and that its processing therefore falls within the scope of Regulation (EU) 2016/679, the next question is how the responsibility for that processing is allocated in practice. This issue becomes particularly complex in the context of smart metering because, unlike more traditional forms of data processing, the electricity system involves multiple actors that all interact with the same stream of consumption data. While the GDPR centralises obligations on the “data controller”, Directive (EU) 2019/944 leaves considerable discretion to Member States in organising data management and defining which parties are entitled to access meter data as “eligible parties”. This creates a structural tension: although the GDPR provides a uniform set of duties, the multiplicity of actors and the diversity of national data management models make it difficult to clearly identify who, in each case, effectively determines the purposes and means of processing and must therefore assume the role of data controller.

In practice, this ambiguity plays out differently depending on the national data management model. In some Member States, the energy supplier is treated as the main data controller because it is the party that has the contract with the consumer and decides what meter data it needs and how it will be used for billing or customer services. In other Member States, however, the role of controller is placed primarily on the Distribution System Operator (DSO), since it owns the grid, installs and operates the smart meters and determines how consumption data are technically collected and managed; in those cases, suppliers may still become additional controllers whenever they use the same data for their own purposes, such as invoicing or dynamic tariffs. Further complications arise where a central communications entity manages the flow of data between meters, DSOs and suppliers: although it may initially act as a processor, it can become a controller if it decides who can access the data or authorises new uses of it. Likewise, energy regulators and third-party service providers that receive meter data for policy analysis or value-added services may also qualify as controllers. This multiplicity of actors explains why, despite a single General Data Protection Regulation framework, the practical allocation of controller responsibilities varies across Member States.

Identifying if an actor classifies as a controller or processor is key because the responsibility they hold varies tremendously. According to Article 4 of the Regulation the “controller” is the natural or legal person, public authority or agency responsible for processing personal data and determining the purposes and means of the processing of personal data. While the “processor” is an actor who processes the data of the data subject on behalf of the controller. Overall the controller is ultimately responsible for the processor’s data processing, but in the electricity sector determining who will be the processor is dependent on the managing model of each Member State. With uncertainty about which actor from the electricity sector corresponds to the roles assigned according

to the data protection framework, it is harder for data subjects to exercise their rights (Baumgart & Espinoza, 2024). Once a data controller is identified in the smart metering context, that actor is subject to the core obligations of Regulation (EU) 2016/679. This means that any processing of consumption data must comply with the Regulation principles of lawfulness, purpose limitation, data minimisation, security and accountability, and that appropriate technical and organisational measures, including data protection by design and by default, must be in place. The controller must also carry out a data protection impact assessment where the processing entails high risks for individuals, as is typically the case with smart meter data.

A final remark to be made regarding the complication of accurately identifying the relevant actor when it comes to smart metering systems concerns the legitimacy and lawfulness for processing the data. Crucially, because the controller determines the purposes and means of processing, those purposes can only be legitimate if they rely on one of the lawful bases in Article 6 of the Regulation, finding the adequate ground being a challenge itself, sometimes leading to discussions around the use of the data subject's informed consent for certain forms of processing. It is most likely that when the data subject accepts to be provided a service they have had the opportunity to consent to the processing of their data, which in any case the data controller must ensure is a fully informed decision. There are also additional grounds for processing the data, most notably that it may be necessary for the performance of a contract or for compliance with a legal obligation. Smart meter data can be processed by multiple actors for multiple purposes, thus a different ground for processing is required for each specific purpose.

However focusing on consent, the use of smart meters creates the difficulty of identifying who is the data subject, because they have to grant consent for processing the data or for eligible parties to have access to the data but when smart meters collect data of more than one individual (because they are installed for instance in a household), the direct identifiable individual would be the one contracting with the energy company, but the collection and analysis of the smart meter data can result in the identification of other individuals residing in that household (Baumgart & Espinoza, 2024). From the perspective of Regulation (EU) 2016/679 any person that can be identified or is identifiable is a data subject and therefore in principle can exercise their rights as such. The question of what would happen if only one or a few people wish to give consent for the processing of their data living within the same household is unresolved by the general data privacy framework. This ultimately does not mean that the GDPR was not designed to address technological developments. On the contrary, its horizontal and principles-based nature allows it to apply across a wide range of contexts. However, the case of smart meters shows that certain highly data-intensive sectors require more specific, sectoral rules that operate alongside the general framework. In these areas, greater regulatory concretisation is necessary to ensure that the GDPR can be applied in a more effective, predictable and user-friendly way, so that individuals' rights and privacy are genuinely protected in practice rather than only in theory.

II. The Commercial Potential of the Processing of Energy Consumption Data

The tensions outlined in the previous section become even more pronounced when smart meter data is not only viewed as something that must be protected, but also as an economic resource with potential market value. While Regulation (EU) 2016/679 is primarily concerned with safeguarding individuals' right to privacy, it simultaneously promotes the free movement of personal data within the Union, subject to its rules. This objective appears to converge with the Union's more recent strategy of developing a data-based market in which data is treated as an economic asset that can be repurposed and shared to enable new forms of economic activity. Moreover, beyond personal data strictly speaking, smart metering systems generate large volumes of information that fall outside the scope of the General Data Protection Regulation, particularly data relating to commercial and industrial facilities, which can be highly valuable despite not referring to natural persons.

In any case, whether personal or not, smart meter data has significant commercial potential. Beyond obvious uses in marketing and advertising, a range of actors may have legitimate interests in accessing detailed consumption information. For example, energy service providers could rely on such data to design more efficient tariffs or personalised energy-saving services that ultimately benefit consumers through lower costs or improved grid stability. Against this background, and in light of the emerging European data economy that increasingly treats energy data as a tradable and reusable asset, it becomes necessary to move from the question of how smart meter data should be protected to how it can legitimately circulate within the European data market.

II.I Data Act

As seen throughout this article, smart meters and the data they produce are not governed by a single harmonised framework in the European Union. Instead, access to and sharing of meter data require consideration of several overlapping legal instruments. In this context, the recently adopted Regulation (EU) 2023/2854 (Data Act) becomes particularly relevant to examine.

The main objective of the Data Act is to give individuals and businesses greater control over data generated through the use of Internet of Things devices, termed "connected products". Importantly, the Data Act is a horizontal instrument and does not displace sector-specific legislation characterised as *lex specialis*, such as Directive (EU) 2019/944 and Implementing Regulation (EU) 2023/1162, which already establish a detailed scheme for meter data access. This is confirmed in Article 44 of the Data Act, which provides that pre-existing EU data obligations remain unaffected and that the Act does not prevent the application of specific sectoral requirements. Nevertheless, the relationship between electricity legislation and data legislation remains complex, and the same difficulties in identifying the relevant actors reappear here, just as they did in the context of personal data under Regulation (EU) 2016/679. A further complication lies in the absence of consensus on whether the Data Act actually applies to electricity metering. As Nicolai

and Münchmeyer observe, there is still considerable uncertainty and limited doctrinal analysis on this issue. Some authorities consider that smart meters fall directly within the scope of the Act, while others argue that the existing electricity framework is sufficiently comprehensive to leave little room for the application of a general sharing regime.

The Data Act applies to data generated by “connected products”, defined in Article 2(5) as “an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user” Difficulties arise when trying to determine whether smart meters truly generate data about their “environment”, since they primarily measure electricity consumption rather than producing data about the device itself. Additional complexity stems from the definition of “user” defined in Article 2(12) which refers to the natural or legal person who owns the connected product or has contractual rights to use it. In the smart metering context, the electricity consumer is not necessarily the owner of the meter under Directive (EU) 2019/944, and although a fee for the meter is often included in the electricity bill, this is not always legally characterised as a rental or usage charge in all Member States. As a result, consumers do not always fit neatly within the Data Act’s definition of “user”, which complicates their ability to rely exclusively on its data access and sharing provisions.

Nevertheless, assuming that the Data Act applies to smart meter data sharing, it should be understood as complementing rather than replacing EU electricity legislation. The Interoperability Implementing Regulation (EU) 2023/1162 under Directive (EU) 2019/944 already provides the most detailed sectoral rules on how data should be shared with eligible parties, clarifying roles and establishing practical procedures for near real-time data flows, access to historical data, and the revocation of permissions, all of which are central for the possible development of commercial usage of smart meter data. The Data Act, however, adds an additional horizontal layer of protection that operates alongside the electricity framework. It does so by placing clearer limits on how third parties may use smart meter data once they have access to it, requiring that the data be processed strictly for the purposes agreed with the user and preventing its reuse for unrelated or intrusive practices such as profiling. At the same time, it strengthens users’ control over their data by increasing transparency about how metering devices operate, what data is shared, and how individuals can access or erase it. Crucially, unlike the Electricity Directive, the Data Act also establishes an explicit right for individuals to lodge complaints before national competent authorities if they consider that their rights have been infringed, thereby providing a more direct and structured enforcement mechanism.

Even if smart meter data holds significant economic potential beyond its direct role in energy efficiency and consumer optimisation, the current regulatory landscape makes it

difficult for market actors to fully exploit that potential. In the absence of clear legal certainty on how the Data Act applies to smart metering, and given the already complex interplay between energy and data protection law, it is unlikely that companies will be willing to invest heavily in new data-driven products or services. At present, the Implementing Regulation (EU) 2023/1162 remains the main sector-specific framework governing data sharing in the electricity sector, but it must be applied in conjunction with Regulation (EU) 2016/679 (GDPR) whenever personal data is involved, and now also alongside the Data Act, at least until its scope is more clearly defined.

Conclusion

This article has shown that smart meter data occupies a particularly difficult position within the current EU legal framework. It is not simply technical information about electricity consumption what smart meters collect, but highly granular personal data that is at the same time indispensable for the functioning of digital electricity grids and for the broader energy transition. This dual character explains why its governance cannot be neatly addressed either by energy law alone or by data protection law alone.

From the analysis developed throughout this work, it becomes clear that the central problem is not the absence of rules. Smart meter data is already covered by a dense regulatory framework that includes Regulation (EU) 2016/679 (GDPR), EU electricity legislation and, potentially, Regulation (EU) 2023/2854 (Data Act). The obligations laid down in these instruments are, in themselves, clear. However, when they are applied to a complex, multi actor electricity system with different national models of data management, serious difficulties emerge at the level of implementation.

In particular, the main challenge lies in identifying who is actually the addressee of those obligations in practice. In a fragmented electricity ecosystem involving suppliers, distribution system operators and intermediaries, it is often unclear which actor truly determines the purposes and means of processing, being possible multiple processings happening at once. As a result, consumers do not lack rights, but they frequently lack clarity about against whom those rights should be exercised.

At the same time, smart meter data is increasingly treated as an economic resource within the emerging European data economy, even though it remains deeply personal in nature, particularly for households data. This generates a structural tension between the objective of facilitating data sharing and innovation and the need to protect individuals' privacy. The uncertain applicability of Regulation (EU) 2023/2854 to smart meters illustrates this problem, since it does not fully clarify how its logic of data access fits with existing electricity and data protection regimes.

Overall, the current framework is not incorrect, but it is insufficiently tailored to the specific reality of smart metering. Regulation (EU) 2016/679 offers strong protection in principle, and Directive (EU) 2019/944 establishes important rules for electricity data, yet neither framework fully reflects the institutional complexity of the sector. What is

needed is greater sectoral concretisation that clarifies roles, responsibilities and access conditions without weakening privacy protection.

Finally, this legal issue cannot be separated from the climate context. Smart meters are essential for digital grids and large scale electrification, and their data will only grow in importance for decarbonisation. If governance remains fragmented and unclear in practice, both effective privacy protection and the innovative use of energy data necessary for the energy transition risk being hindered.

References

Baumgart, M & Espinosa Apráez, B 2024, On the implementation of smart meters in the European Union : Legal considerations regarding privacy and personal data protection in times of the Twin Transitions. in R Leal-Arcas (ed.), Research Handbook on EU Energy Law and Policy. 2nd edn, Research Handbooks in Energy Law series, Edward Elgar Publishing, Cheltenham, pp. 500-526. <https://doi.org/10.4337/978>

Beckel, C., Sadamori, L., Staake, T., & Santini, S. (2014). Revealing household characteristics from smart meter data. *Energy*, 78, 397-410. <https://doi.org/10.1016/j.energy.2014.10.025>

Directory, S. (2025, 28 noviembre). Why Is Smart Meter Data Privacy Important? Question. Energy Sustainability Directory. <https://energy.sustainability-directory.com/question/why-is-smart-meter-data-privacy-important/>

E.DSO, 'Feedback to Data Act' (2022) www.edsofsmartgrids.eu/content/uploads/2024/05/E.DSO-feedback-to-Data-Act.pdf

European Commission: Directorate-General for Energy. (2024). Electricity metering and consumption data interoperability : guidance for the reporting of national practices in accordance with Commission Implementing Regulation (EU) 2023/1162. Publications Office of the European Union. <https://data.europa.eu/doi/10.2833/34389>

Kashyap, S., Schwinger, W., Grünberger, S., Schaffer, C., & Hartner, G. (2025). Energy data governance fragmentation in Europe: challenges, models, and pathways to integration. EDDIE: European Distributed Data Infrastructure For Energy, 1-6. <https://doi.org/10.1109/eem64765.2025.11050331>

Kashyap, S., Schwinger, W., Grünberger, S., Schaffer, C., & Hartner, G. (2025, May). Energy Data Governance Fragmentation in Europe: Challenges, Models, and Pathways to Integration. In 2025 21st International Conference on the European Energy Market (EEM) (pp. 1-6). IEEE.

Lavrijssen, S.; Espinosa Apráez, B.; ten Caten, T. The Legal Complexities of Processing and Protecting Personal Data in the Electricity Sector. *Energies* 2022, 15, 1088. <https://doi.org/10.3390/>

- Lee, D., & Hess, D. J. (2021). Data privacy and residential smart meters: Comparative analysis and harmonization potential. *Utilities Policy*, 70, 101188. <https://doi.org/10.1016/j.jup.2021.101188>
- Menges, L. (2024). Climate change and state interference: the case of privacy. *Philosophical Studies*, 182(2), 425-443. <https://doi.org/10.1007/s11098-024-02269-6>
- Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). Private memoirs of a smart meter. *ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings*, 61–66. <https://doi.org/10.1145/1878431.1878446>
- Nicolai, S., & Münchmeyer, M. (2025). The EU Data Act and electricity consumer participation in demand response and flexibility services. *Journal of Energy & Natural Resources Law*, 1–25. <https://doi.org/10.1080/02646811.2025.2485725>
- Opinion 1/2010 on the concepts of “controller” and “procesor”. (2010). Article 29 Data Protection Working Party https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
- Opinion 12/2011 on smart metering. (2011). Article 29 Data Protection Working Party. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf
- Peers, S. (2018). Data protection and smart meters: the GDPR and the ‘winter package’ of EU clean energy law. <https://eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html>
- Rieman, R. & Information Technology Policy Unit of the European Data Protection Supervisor. (2019). TechDispatch #2: Smart Meters in Smart Homes. En European Data Protection Supervisor (N.o 2). <https://doi.org/10.2804/87340>
- Security and Privacy in the Smart Grid. (2021). [PHD thesis, Radboud University]. <https://www.polvanabel.com/research/phdthesis/phd-thesis-pol-van-aubel-security-and-privacy-in-the-smart-grid-2023-08-24.pdf>
- Sharma, A., Sangal, A. L., & Sharma, K. C. (2025). Privacy-preserving prosumer profiling using smart meter data. *Sustainable Energy Grids And Networks*, 43, 101784. <https://doi.org/10.1016/j.segan.2025.101784>
- Smart Grids: from innovation to deployment. (2011). Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions Smart Grids: from innovation to deployment (N.o 52011DC0202). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0202>

Legislation

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC

Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) (Text with EEA relevance.)

Commission Implementing Regulation (EU) 2023/1162 of 6 June 2023 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)