Chapter 1
Responsible and Safe Home Metering: How to Design a Privacy-Friendly Metering System

Libor Polčák
Brno University of Technology, Czech Republic

ABSTRACT

The European directive on energy efficiency requires that all meters in multi-apartment buildings installed after 25 October 2020 shall be remotely readable devices when technically feasible and cost-effective in terms of being proportionate to the potential energy savings. The European Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU) explicitly mentions that smart metering predominantly processes personal data. This chapter recommends how to design a metering system that fully conforms to legal regulations. The main contribution is the recommendation of eight steps for data controllers that make metering systems legally compliant. Additionally, the chapter lists recommendations for smart meter manufacturers that remove the burden of being a controller of the processing. The recommendations apply to the distribution of electricity, water, gas, heat, cooling, and other energies. The chapter shows that the recommendations can be generalized for smart home deployments.

INTRODUCTION

The European Union (EU) takes the impact of people on the environment seriously. Previous research has shown that transparent energy metering can reduce consumption (March et al., 2017; Kaatz, 2017; Beal & Flynn, 2015; Liu et al., 2015). Moreover, meters can detect tampering (Monedero et al., 2015) and water leakage (Britton et

DOI: 10.4018/978-1-6684-5991-1.ch001

al., 2013, Lima & Navas, 2012). Consequently, the current text of the EU directive on energy efficiency mandates the deployment of remotely readable and cost-effective provisioning of billing and consumption information for heating and cooling and domestic hot water for each building unit, where technically feasible and cost-effective in terms of being proportionate in relation to the potential energy savings (Directive Articles 9b (1) and 9c; European Parliament and Council, 2018).

The EU Directive on common rules for the internal electricity market provides requirements for smart metering systems (Directive 2019/944/EU, Article 20; European Parliament and Council, 2019). Specifically, the consumption data need to be available securely: "the security of the smart metering systems and data communication shall comply with relevant Union security rules, having due regard of the best available techniques for ensuring the highest level of cybersecurity protection while bearing in mind the costs and the principle of proportionality" (Directive 2019/944/EU, Article 20(b); European Parliament and Council, 2019). "The privacy of final customers and the protection of their data shall comply with relevant Union data protection and privacy rules" (Directive 2019/944/EU, Article 20(b); European Parliament and Council, 2019). Nevertheless, the deployment of smart metering for electricity metering is not mandatory and should be decided by each EU member state through an assessment (Directive 2019/944/EU, Article 19(2); European Parliament and Council, 2019).

A well-designed metering system can help to reduce energy consumption. However, current literature also highlights that the success of metering systems depends on their security (Kumar et al., 2019). As energy distribution is considered critical to our societies, smart metering network operators and manufacturers should consider robust security and privacy features from the beginning (Kumar et al., 2019). Poorly designed metering systems risk incompatibilities with data protection laws (Polčák & Matoušek, 2022). Cuijpers & Koops (2012) describe the failure of smart metering deployment in the Netherlands due to detailed readouts; the proposed Dutch law supposed processing data that were not minimized and not necessary. The main goal of this chapter is to assist in designing metering systems conforming to the data protection law. Data protection authorities can ban a metering system that unlawfully processes personal data or issue an order to redesign the system. Such a ban or a redesign would increase the cost of the deployment. Recall that the EU law mandates balancing the metering system deployment based on the costs and its potential for energy savings. Hence, this chapter aims to provide advice on the requirements stemming from data protection laws to assist in designing a metering system correctly from the beginning.

This chapter focuses on legal requirements for remotely readable metering systems. The research methodology is as follows. The author of this chapter researched the cases of the Court of Justice of the European Union (CJEU) concerning data protection issues together with the guidance of the European Data Protection Board (EDPB) and its predecessor Article 29 Data Protection Working Party concerning EU General Data Protection Regulation 2016/679/EU (GDPR, European Parliament and Council, 2016) requirements, smart metering, and other related topics like the Internet of things. Additionally, the chapter's research methodology involved studying research papers on privacy and security issues in smart metering. The research also considered smart metering data protection development in the United States and Canada. In summary, this chapter does not propose any new metering system. Rather, this chapter brings together data protection law requirements and applies them to metering systems in general. The requirements are applicable from small deployments to deployments spanning countries; considered metering systems involve electricity, water, gas, heat, cooling, and other energy distribution systems.

The text of the chapter argues that data processed by the metering systems are often personal data. Hence, European Parliament and Council (2016) (General Data Protection Regulation, GDPR, Regulation 2016/679/EU) typically applies. Consequently, the requirements of European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) on controllership, data minimization, transparency, and fairness must be fulfilled. Moreover, the chapter provides suggestions on architecting and deploying metering systems that fully conform to law requirements. To facilitate the understanding, the chapter introduces multiple scenarios of possible smart metering systems, ranging from a small deployment without a permanent reading infrastructure to a full electricity smart grid. Finally, the chapter generalizes the requirements for smart homes.

BACKGROUND

This section introduces key terms related to advanced energy consumption metering. Later, this section focuses on the data protection issues connected with remotely readable metering systems from the law position and reviews related work.

Terminology Related to Metering Systems and Smart Grids

There is not a single type of a metering system. Some are deployed in a single building, whereas others span a whole country. A smart electricity grid typically consists of many heterogeneous systems (Kumar et al., 2019, Knap & Samani, 2013). In contrast, remote readout also covers meters periodically transmitting metering data without any permanent reading infrastructure (Polčák & Matoušek, 2022).

- **Automatic Metering Readout (AMR)** allows only communication initiated by the meters and often without the possibility of sending data to the meter. The meters are typically not directly connected to a wired network and are powered by batteries. The goal is to minimize the power requirements of the meter. To do so, the meter does not listen for any incoming transmissions. Instead, the meter sends readouts during predefined intervals (e.g., periodically). These messages might be processed either by an occasionally available device or a permanent infrastructure.
    - **Readings by an occasionally available device:** These readings need a reading service that periodically reads the meters by visiting the building or reading the readouts from a car parked in the vicinity of the building. Hence, there are no additional costs for permanent reading devices (e.g., gateways between the metering protocols and the internet protocol suite TCP/IP), and it is not necessary to provide a durable connection to the internet. Such deployment is suitable if the only goal is to provide billing information, but it is impossible to provide real-time information on events like water leakage. However, a meter can detect events such as attempted fraud. Nevertheless, the reading service would learn about the incident with delay.
    - **Readings by a permanent infrastructure:** As the battery-powered meter's signal typically spans only tens or hundreds of meters and the data need to be processed across a city or a country, a permanent architecture composed of gateways can relay the readings to a different medium. For example, data can be aggregated from all local meters and relayed to the metering facility over the internet. As the metering facility can process the data in real time, it can timely react to detected events, such as suspected fraud or water leakage. All data from a meter can be analyzed and evaluated by the reading facility if the customer wishes to benefit from the detailed information on energy consumption, for example, to learn about activities that result in very high consumption.
- **Advanced Metering Infrastructure (AMI)**, also called **smart grid**, for example, by Kumar et al. (2019). Mohassel et al. (2014) and Knapp & Samani (2013) describe AMI thoroughly. The infrastructure is heterogeneous and hierarchical; it includes smart meters, communication networks, data management systems, and means to integrate collected data into software platforms and interfaces. AMI allows bidirectional communication, typically initiated by the infrastructure. AMI does not need meters that send data periodically. Instead, the infrastructure begins each readout. Typical AMI meters allow advanced features to improve the reliability, efficiency, and sustainability of the grid. For example, connected devices can negotiate with

the network the optimal time to consume resources (for example, to charge an electric vehicle during the night). AMI allows for negotiation of providing energy back to the network, for example, from solar panels mounted on residential buildings.

Remote readouts may be employed for different purposes (Kumar et al., 2019; Knapp & Samani, 2013):

- **Metering for billing** performs the same functionality as legacy analog metering. The goal is to meter consumption and issue a bill.
- **Metering for operations** is used to optimize the efficiency and reliability of the network. For example, the utility company may analyze patterns in energy consumption and predict future workload.
    - Cuijpers & Koops (2012) mention remote energy quality detection, the ability to turn the power supply off to deal with fraudulent or nonpaying customers and to deal with disasters.
    - Accident detection is another operational example. Britton et al. (2013) claim that current estimations assume customer postmeter leakage accounts for up to 10% of total water consumption, particularly in the residential sector. They report significant water savings resulting from the early detection of household leaks. Smart metering provides water utilities with a powerful tool to identify rapidly and take action in case of a postmeter leakage.
- **Value-added services** let the user benefit from smart metering. For example, the user can receive suggestions on how to improve energy consumption (Chen et al., 2011), or the smart grid may instruct cooperative appliances in the household to use electricity at low prices during off-peak times (Knapp & Samani, 2013).

Smart metering systems typically employ protocols like ZigBee (IEEE 802.15.4), Z-wave, Wi-Fi (IEEE 802.11), MobileFi (IEEE 802.20), WiMAX (IEEE 802.16), powerline communication (PLC), mesh networks on unlicensed radio, and Wireless M-Bus (Kumar et al. 2019; Brunschwiler, 2013). Concentrated data are sometimes carried over the internet using TCP/IP (Kumar et al., 2019).

RELATED LITERATURE

Orlando & Vandevelde (2021) focused on the EU law and found the EU approach correct but not optimal. They think that personal data should be collected for the public interest (as the GDPR legal basis); they highlight several requirements of the law, such as identifying the entities, such as data subjects, controllers, and processors. Knyrim & Trieb (2011) also highlight the need to base the deployment on legal bases other than consent. Lee & Hess (2021) compared privacy regulations of smart residential meters in Canada, France, the Netherlands, Norway, the United Kingdom, and the United States. They identified strategies that help gain public confidence: (1) opt-out policies for mounting a smart meter, (2) opt-in policies for provisioning of highly granular data that allow identification of activities, (3) rules for data storage and data sharing, and (4) independent monitoring and supervision on privacy-related practices.

As discussed above, metering systems differ in complexity. Hence, each deployment may result in a different set of threats. Kumar et al. (2019) offers an overview of the threats appearing in the metering systems, including advanced persistent threats, targeted attacks, privacy issues, denial of service radio subversion, credential compromise, illegal access, message modification, man-in-the-middle attacks, data analysis, misuse of private data, routing attacks, meter compromise or intrusion, location migration, and cloning. The threats endanger individuals (customers), the metering systems, and the ability of utilities to distribute energy. According to Kumar et al. (2019), privacy threats are not fully understood in the metering systems. An attacker can be an insider or an outsider, the attackers can connect directly to the network, or they can use logical access through insecure components and other means (Kumar et al., 2019).

Chen et al. (2011) showed that readouts with 15-minute periods reveal household activities, such as taking a shower or using a washing machine or dishwasher. Some devices have a distinct pattern of energy consumption that can be used to fingerprint a device (Lisovich et al., 2010; Kelly & Knottenbelt, 2015). Consequently, a remote adversary can reveal the manufacturer or even the model of household appliances without ever entering the household. Such information is convenient for burglars, profiling, and marketing (Kumar et al., 2019; Polčák & Matoušek, 2022).

A related issue is zero-consumption detection. Energies like water or gas are typically not used in an unoccupied property. Even though some electrical appliances can run in standby mode, the electricity consumption in an unoccupied property generally is much lower compared to the periods when the property is occupied. Erol-Kantarci & Mouftah (2013) and Lisovich et al. (2010) point out the risks.

Several privacy-enhancing techniques deployable by residents appeared in the literature. Backes & Melser (2012), Kalogridis et al. (2010), McLaughlin et al. (2011), Yang et al. (2012), Armel et al. (2013), Zeifman & Roth (2011) mention a battery mounted after a smart electricity meter at the edge of the household grid. Such a battery hides peaks in energy consumption with an almost constant charging current. However, the battery approach is expensive when applied to hide occupancy patterns, so Chen et al. (2014) proposed preventing occupancy detection using the thermal energy storage of large elastic heating loads already present in many homes, such as electric water and space heaters. Orlando & Vandevelde (2021) question if such approaches are an obstacle to the potential of smart meters in terms of benefits. Specifically, both batteries and heaters in unoccupied flats waste (some) energy.

Rial et al. (2018) propose a sophisticated approach that encrypts metered data with a key shared with the residents. Later, residents need to: (1) decrypt the metered values on their devices and (2) compute costs. The approach ensures that the utility can verify the cost computation. Moreover, Rial et al. (2018) also propose extensions for future demand predictions, fraud detection, and profiling. However, Kumar et al. (2019) argue that it is widely accepted that public and private key-based mechanisms are considerably expensive concerning computational complexities.

Homomorphic encryption allows to encrypt and share information between multiple parties in a way in which arithmetic operations can be done on encrypted data without the need to decrypt the data first. Abreu & Pereira (2022) note that two main disadvantages of homomorphic encryption for smart grids are its complexity and that meters are not independent. Using homomorphic encryption, it is possible to aggregate data from multiple meters without revealing the specific consumption of the meters to the metering facility.

Kumar et al. (2019) show that encryption-related issues are an open topic in current literature. Symmetric encryption is fast but needs a complex key management solution. Asymmetric keys simplify key management but suffer from bad performance on resource-hungry devices. Homomorphic systems and public key infrastructure are often too expensive, especially considering battery-powered devices (Esposito & Ciampi, 2015; Kumar et al., 2019). Homomorphic encryption generates larger messages (Esposito & Ciampi, 2015; Kumar et al., 2019).

Smart meters are often wireless (Kumar et al., 2019). Consequently, they suffer from jamming and spoofing attacks (Kumar et al., 2019; Polčák & Matoušek, 2022; Brunschwiler, 2013). The mitigation of this threat is through detection techniques that create alerts, and the misbehaving devices can be identified (Kumar et al., 2019). A metering system can mitigate a replay attack with enforced integrity detection. For example, Polčák & Matoušek (2022) describe an attacker that can store metering messages and replay them later to lower the bill. Although the studied system tracked time in the metering messages, it did not use the time stamp to detect integrity violations.

Comparison to this chapter: The related work identified many relevant problems and solutions. However, none of the work provides a clear set of instructions that can be followed by the parties participating in the smart metering and manufacturers of the smart meters. Rial et al. (2018) proposed a privacy-preserving approach that was tested by real utilities. However, this chapter provides more general guidance.

Following the guidance, one can be determined that the proposal of Rial et al. (2018) fulfills data protection requirements. However, other architecture and deployments that are not based on Rial et al. (2018) are also compliant. Orlando & Vandevelde (2021) focused on the law and what is missing, but they do not give detailed technical guidance. This chapter generalizes the advice given by Polčák & Matoušek (2022). Their advice considers a specific deployment. In contrast, this chapter focuses on metering systems in general.

EU Data Protection Law and Rules

The fact that metering systems process personal data is a well-established concept in the literature (Lee & Hess, 2021; Orlando & Vandevelde; 2021; Knyrim & Trieb, 2011). This section focuses on the interpretation of the regulatory bodies. Orlando & Vandevelde (2021) cover the history of soft law that has clarified crucial aspects. The European Commission set up a task force related to smart grid operations; one group consisted of European data protection authorities (DPAs) established in all member states. These authorities were grouped in the Article 29 Data Protection Working Party (GDPR transformed the working party into EDPB). The Article 29 Data Protection Working Party (2011) produced its Opinion 12/2011, expressing its view that metered data are often personal data.

The European Commission applied the Article 29 Working Party Opinion (2011) (Opinion 12/2011) on smart metering to the Commission Recommendation of March 9, 2012 (European Commission, 2012) on preparations for the roll-out of smart metering systems (2012/148/EU, European Commission, 2012). Through Programming Mandate M/487 EN, the European Commission (2011) also asked the European Standard Bodies to revise and secure standards for smart metering. Even though the standards were revised, some literature provides evidence that the revised standards were not always implemented in practice (Polčák & Matoušek, 2022). Nevertheless, Commission Recommendation is not legally binding. However, data protection regulations like European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) are legally binding.

The Recommendation 2012/148/EU (European Commission, 2012) states in recital 6 that “Smart metering systems allow processing of data, including predominantly personal data.” The author of this chapter adds that smart metering is also deployed in factories and other industrial deployments. Additionally, smart metering is deployed in public buildings, hotels, and other facilities where the measured data are aggregated for the whole building or even a campus. Hence, not all data are personal. Recital 30 of European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) recognizes that identifiers provided by devices may be used to identify them. Moreover, the CJEU (2016) (in Case C-582/14) considered a dynamic IP address personal data, provided that there are reasonable means that can be used to identify the person.

Recitals 10 and 11 of the Recommendation 2012/148/EU (European Commission, 2012) clarifies European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU, Article 25) on data protection by design and by default: "security features should be built into smart metering systems before they are rolled out and used extensively. Such features can effectively improve consumers' control over the processing of personal data." National data protection authorities should stimulate the principle in the early phases of the roll-out.

European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) deals with data protection impact assessment in Article 35. Recital 15 of the Recommendation 2012/148/EU (European Commission, 2012) argues that an assessment of the data protection impact should be carried out prior to the roll-out of smart metering systems. European Commission (2014) (Recommendation 2014/724/EU) later clarified the requirements for data protection impact assessment.

European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) lists several obligations. Article 4 provides definitions for basic terms like personal data, processing, controller (the entity that decides the means and purposes of the processing), and processor (an entity that processes personal data on behalf of the controller). Article 5(1) declares the basic rules for processing: lawfulness, fairness, and transparency, and Article 5(2) puts restrictions on the processing like purpose limitation and data minimization; the controller is responsible for the demonstration of compliance (accountability principle). Article 6 provides legal bases for processing (note that all except consent allow processing only strictly necessary personal data).

CJEU (2010, 2013, 2014, 2017, 2019a) decided several cases that dealt with the condition of necessity (C-92/09 and C-93/09, point 86; C-473/12, point 39; C-212/13, point 28; C-13/16, point 30; C-708/18, points 40–45). In essence, CJEU is strict on considering what is necessary and what is not. CJEU is also strict on considerations of what is data minimization (see, C-708/18, points 48–51, CJEU, 2019a). Case C-708/18 (CJEU, 2019a) assessed a deployment of a video surveillance system. CJEU decided that as the controller applied less invasive measures before applying more intrusive measures, the controller fulfilled the minimization principle. The lesson to be taken is that it is necessary to try, or at least consider, less privacy-invasive measures before applying more intruding measures.

European Parliament (2021) (Resolution 2021/C 494/11) recently evaluated European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU). In the resolution, the European Parliament "Expresses its concern about the uneven and sometimes non-existent enforcement of the GDPR by national DPAs more than two years after the start of its application, and therefore regrets that the enforcement situation has not substantially improved compared to the situation under Directive

95/46/EC." The author interprets the text as evidence that European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) enforcement is lacking and that many processing activities are not in line with the regulation. According to the resolution, EDPB should adopt guidelines to determine the conditions under which ICT manufacturers should be considered controllers. EDPB did not publish the guidelines yet. One of the contributions of this chapter is to anticipate and manifest what should be in the guidelines.

Cuijpers & Koops (2012) described the failed roll-out of smart metering in the Netherlands as due to the flawed regulations without respecting the law from the beginning. The proposal did not clearly define processing parties and purposes; there was no data protection impact assessment; and the proposal did not respect principles of data privacy by design. Two smart-metering bills expected mandatory roll-out for every household with 15 minutes readout periods for electricity and hourly readouts for gas. Energy suppliers were supposed to derive detailed information about energy consumption so that consumers could adapt their behavior for greater efficiency. The meters were supposed to cut out the household from the energy supply for fraudulent behavior and nonpayers. The Dutch Senate blocked the two bills in 2009 due to privacy concerns. Privacy concerns led to the Dutch Data Protection Authority being asked to give advice on the bill. The authority raised concerns about the lack of legitimate processing basis opaque access to the personal data of different parties. Consequently, the proposal was amended: (1) to require explicit consent to transfer the frequent readouts, (2) daily readouts would be mandatory, and (3) all data protection conditions like purpose limitation or data subjects' rights would apply. The authority deemed the legislation compliant with the Dutch Data Protection Act.

Nevertheless, the Dutch Consumer Union let Cuijpers & Koops (2008) evaluate the bills in the light of Article 8 of the European Convention on Human Rights (ECHR) Article 8. The report concluded that: (1) the processing of quarter-hourly and hourly readings to grid managers, (2) the daily readings to grid managers and suppliers, and (3) the compulsory roll-out of smart meters to all households were not (proven to be) necessary in a democratic society and the roll-out would violate ECHR (Cuijpers & Koops, 2012). Additionally, the report found that the government provided too little evidence to assess the necessity of the built-in switch that was supposed to cut out the household from the energy distribution remotely, as it introduces new opportunities for abuse, for example, by remote adversaries (Cuijpers & Koops, 2012).

The text of the law was updated by: (1) improving the coherence of the management of end-user data by the parties involved, (2) improving transparency and awareness by requiring the publishing of annual reports on the processing, (3) the smart meters were no longer obligatory, and (4) the law explicitly refined purposes of processing, such as billing and network management. The law passed in 2011 (Cuijpers & Koops, 2012). In summary, the roll-out was delayed by several years, and the final rules significantly changed. Zhou & Brown (2016) described the Netherlands as a laggard in smart meter deployment.

Zhou & Brown (2016) compared smart meters deployment in Finland, Sweden, Denmark, Germany, and the Netherlands. Finland and Sweden have a high smart meter deployment ratio, while Germany and the Netherlands have a low deployment. Interestingly, Zhou & Brown (2016) mention only Germany and the Netherlands as countries with opposition from the public due to privacy and security concerns. However, Germany was the only country with a negative cost-benefit analysis that resulted in the reported adoption slowdown. Nevertheless, Finland specified purposes for processing, obligations for data transmissions and storage, data security and protection, and rights for data subjects. The desire of accurate billing mainly drove deployment in Sweden. Although Sweden does not require smart metering, the requirement for monthly readings lets the market select smart metering as the optimal path.

Orlando & Vandevelde (2021) researched the Flemish (a part of Belgium) implementation of electricity distribution. The Flemish Regulator of the Electricity and Gas Market has to publish regular reports to the public and government. The law lists specific cases with mandatory digital meters and specifies the processing of metering data which provides a legal basis under Article 6(e) European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU). The law limits the purposes of processing. The law specifies legal roles, including defining conditions under which a controller can employ a processor. Finally, the law creates specific rules for risk management and conducting data protection impact assessments, further clarifying Articles 32 and 35 of European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU).

Table 1 summarizes the papers of Orlando & Vandevelde (2021), Cuijpers & Koops (2012), and Zhou & Brown (2016). The lesson learned is that public scrutiny or obliging the principle of privacy by design leads into detailed conditions and regulations provided by law. As European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) is generic, laying down specific criteria in sector law removes some burden from the controllers. Most countries decided on improved transparency and specifying data rights for customers.

Let us compare the European status to the United States. California established the 15/15 rule (Lee & Hess, 2021; Kaatz, 2017) that allows a utility to share data if it aggregates 15 or more customers and if each customer comprised less than 15% of the group's aggregated consumption (California Public Utilities Commission, 2014). New York State Public Service Commission (2018) adopted a 4/50 rule meaning a minimum of four households, each accounting for less than 50% of the total consumption. Orlando & Vandevelde (2021) think that providing such a threshold that is well reasoned would be beneficial for European utility companies. After specifying concrete numbers that make aggregated personal data anonymous and, hence, not protected by data protection rules, the controllers would not need to evaluate their anonymization techniques. A future research question is selecting the number of households and maximum household consumption so that it is guaranteed that a household cannot be reidentified.

Table 1. Comparison of privacy and security-related forces that enables the smooth deployment of smart metering

Country/region	Finland	Sweden	Denmark	Germany	Netherlands (after public scrutiny)	Flanders
Clear specification of roles	Yes	No	Unknown	Unknown	Yes	Yes
Clear list of operations	Yes	No	Unknown	Unknown	Yes	Yes
Mandatory deployment	Unknown	No	Yes	No, negative cost-benefit analysis	Opt-out	Under specific circumstances
Additional transparency requirements	Unknown	No	Unknown	Unknown	Annual reports of processing	Yes
Specific security obligations	Yes	No	Unknown	Yes	Yes	Yes
Specific data rights for customers	Yes, for example, data access	No	Yes, for example, data access	Yes, choose a third party to operate the metering point	Yes, for example, setting the period of readouts	Yes, for example, data access rights, identification of personal data
Assessed by data protection authority or other bodies	Unknown	Unknown	Unknown	Unknown	Yes	Unknown

Note. Data acquired by Orlando & Vandevelde (2021), Cuijpers & Koops (2012), and Zhou & Brown (2016).

In the US case of Naperville Smart Meter Association v. Naperville, the Seventh Circuit Decision (2018) overturned the lower court decision based on previous decisions on legacy analog meters. The Seventh Circuit court stated that:

Using traditional energy meters, utilities typically collect monthly energy consumption in a single lump figure once per month. By contrast, smart meters record consumption much more frequently, often collecting thousands of readings every month. Due to this frequency, smart meters show both the amount of electricity being used inside a *home and when that energy is used (United States Court of Appeals for the Seventh Circuit Decision, 2018, Naperville Smart Meter Association v. Naperville).*

The court decided that the city has an interest in collecting the data in this specific case. Additionally, the city benefited from the policy of not sharing the data without a search warrant or court order. The court has left open a question of readouts with a period lower than 15 minutes. The court also highlighted that the city could have avoided the controversy if they had given the residents the option to avoid a smart meter.

Designing A Smart Metering System

The previous section established that metering systems deployed in residential areas are intrinsically personal data. European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) requires each processing operation of personal data to be proportionate, necessary, and processed personal data to be minimized. As this claim is quite vague, the author will expand this law requirement into several steps that the entities running a metering system (including a smart grid) need to apply. Later, the section focuses on manufacturers of smart meters.

Entity Running a Metering System

Step 1: The controller, the entity planning to run a metering system, has to list all the operations carried out by the planned metering system. Alternatively, a controller can carry these steps during an audit of an existing metering system to determine legal compliance. This step yields a set of operations, such as the need to know the current meter value to provide billing, the need to monitor consumption during a period to detect water leakage, or the analysis of patterns and energy usage to provide suggestions to reduce consumption.

- Note that it is necessary to list all processing operations in advance. The Purpose Limitation Principle prevents controllers from gathering personal data for one purpose, like billing, and later, using the same data for a different purpose. The use for an incompatible purpose is only possible with the consent of the data subject. As the controller might find a different legal basis for additional processing purposes, it is preferable for the controller to list all purposes in advance.

Step 2: The controller must determine the data needed to achieve each selected goal. The controller needs to differentiate between personal data and other data, as personal data requires better protection (Regulation 2016/679/EU, Opinion 05/2014, Article 29 Data Protection Working Party, 2014). The controller should minimize required personal data to the most necessary extent.

- For example, when the law mandates that the controller performs a yearly billing, only one readout is necessary (Opinion 12/2011, Article 29 Data Protection Working Party, 2011). Hence, the frequency of the readouts is directly prescribed in the law in this case.
- The controller can determine that an approach of Rial et al. (2018) or homomorphic encryption can be applied. Consequently, only the customer can access unencrypted data. Orlando & Vandelvelde (2021) note that such an approach does not create anonymous data. However, the author of this chapter thinks that it demonstrates compliance with data minimization, the principle of data protection by design (GDPR, Regulation 2016/679/EU, Article 25, European Parliament and Council, 2016), and the application of technical and organizational security measures (GDPR, Regulation 2016/679/EU, Article 32, European Parliament and Council, 2016). Note that data protection by design refers to the current technological state. Hence, a controller finding that the market does not offer any product detecting necessary events could demonstrate the need to perform frequent readouts to collect data needed to evaluate the events.
- Activities such as fraud detection and water leakage detection need very frequent readouts. Polčák & Matoušek (2022) report meters that perform computations to detect events such as possible fraud or water leakage without requiring frequent readouts to leave the device. There was no court of justice decision directly applicable to this case. However, the author of this text believes that detecting events directly in the meters demonstrates compliance with the principle of data protection by design (GDPR, Regulation 2016/679/EU, Article 25, European Parliament and Council, 2016). Article 29 Data Protection Working Party (2013) (Opinion 05/2013) lists detection of fraudulent activities by mining fraudulent data as compatible with data protection laws, providing that the controller applies safeguards to minimize risks and undue impact on data subjects.
- The controller might need to decide how to reach the same goal from several possibilities. For example, suppose that the controller wants to differentiate between peak and off-peak hours. One option is to read the metered value each time the peak hours start or end. Another option is to deploy a meter that can separately meter consumption for peak and off-peak hours. Note that the latter option allows the controller to read the metered consumption less frequently, demonstrating adherence to the data minimization principle.

Again, the controller can find that there is no suitable meter offering the needed functionality; the wording of the European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU, Article 25) enables the controller to demonstrate that the market does not offer any other meter collecting sufficient data.

- European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) applies only to personal data. The controller should consider the option not to process personal data, for example, for operational processing that does not require personal data but, for example, works with aggregated data. The utility can gather aggregated data in the part of the metering system that carries the energy aggregated during transport before the pipes or wires reach homes and residential buildings or in large substations (McKenna et al., 2012). Article 29 Data Protection Working Party (2014) (Opinion 05/2014) gives examples of anonymization techniques.

Step 3: The controller needs to decide the lawfulness of processing for each selected goal (GDPR, Regulation 2016/679/EU, Article 6, European Parliament and Council, 2016); for example, is the processing a legal obligation, or is it necessary to perform the contract (e.g., differentiate between peak and off-peak hours)?

- The controller can decide to pursue their legitimate interests in the processing—for example, to keep the grid functioning. In such a case, the controller needs to demonstrate that their interests are not overridden by the legitimate interests of data subjects in being private in their homes. In particular, the controller should weigh other possibilities to achieve the same goal.
    - For example, the controller can realize that it does not need the metered value for each household separately to predict future demand. Instead, the controller can employ consumption data from a distribution network that aggregates many households (Knyrim & Trieb, 2011).
    - Another example is to use data from a distribution network composing many households to determine that there is no possibility of fraud in a part of the network. Once a part of the distribution network looks like there might be a fraudulent customer, the controller can decide to collect data from each household in the network segment. The controller should stop processing further data on each household once it establishes that the particular household does not exhibit fraudulent behavior.
- If there is no other possible basis in Article 6 (GDPR, Regulation 2016/679/EU, Article 6, European Parliament and Council, 2016), the controller can decide to offer the service as an added value with the consent of the customer

(each data subject). Such a decision could be reached, for example, by providing detailed graphs about the consumption of the individual household. Such a decision would empower customers to watch their consumption and act accordingly. Not interested in the detailed consumption analysis, other customers could keep their data private. As Orlando & Vandevelde (2021) and Knyrim & Trieb (2011) warn, utilities should avoid the need for consent for operational and billing services of the metering system. The author of this text recommends relying only exceptionally on a consent.

- Suppose the market analysis performed in the second step revealed that the controller needs to deploy a metering device providing more frequent data than necessary. In that case, the controller should reevaluate if the legal basis allows such an interpretation. The more disparity between the absolutely necessary frequency of meter readouts and the actual reading frequency, the more questionable the processing is (Cuijpers & Koops, 2012; Knyrim & Trieb, 2011). Hence, the author of this text recommends depending on more frequent readouts than absolutely necessary, only exceptionally in well-grounded cases.
- The reliance on consent or different contracts (different tariffs, value-added services) may introduce the need for customizable readouts. AMI deployments typically offer the needed customization, but AMR deployments may not be suitable (Polčák & Matoušek, 2022).
- The Article 29 Data Protection Working Party (2013) (Opinion 05/2013) lists transparency, predictability, and user control as related concepts to purpose limitation. The processing must be predictable and sufficiently related to the original purpose of processing. In the case of the metering data, unrelated purposes might be incompatible with legal bases, such as legitimate interests, as the data subject does not predict such processing. In the context of smart metering, unrelated purposes are, for example, marketing activities based on the detected appliances. The data subject interested in getting energy supplies does not suspect automatic profiling of their activities. The Article 29 Data Protection Working Party (2013) (Opinion 05/2013) lists two examples related to smart monitoring:
    - The first example relates to cooperation between tax authorities (for example, to detect occupied flats that are declared unoccupied) or law enforcement (for example, to detect cannabis factories) on one side and the utilities on the other. The Article 29 Data Protection Working Party concluded that such cooperation is possible only under strict conditions of (nowadays) Article 23 of the European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU), that is, there needs to be a legislative measure that respects the essence of the fundamental rights and

  freedoms and is a necessary and proportionate measure in a democratic society to safeguard national security, defense, public security, or other exceptions listed by the Article 23, European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU).
  - The second example is about an analytics tool that detects anomalies in usage patterns. As the controller identifies high risks for data subjects, they consult their plan with regulatory authorities responsible for the electricity grid and data protection (see Articles 35 and 36, European Parliament and Council, 2016) (GDPR, Regulation 2016/679/EU). The controller gets approval for the plan, provided that additional safeguards are in place to minimize the risks of any undue impact on the data subjects like technical and organizational measures, fair and effective procedures to correct any inaccurate results, and transparency towards the data subjects.

Step 4: The controller should decide the envisaged time limits for the collected personal data erasure. For example, the controller is legally obliged to keep (or forward) some data from the smart meters, for example, monthly or yearly readouts. For data collected only for further computation, for example, to detect events, such as water leakage or fraud, the controller can decide that data are needed only for a limited time, sometimes only a fraction of a second. The controller complies with the data minimization principle by processing the data for a minimal period.

Step 5: The controller should reflect other parties taking part during the processing:

- The controller can realize that they want to outsource a part of the processing to another party, for example, because it is cheaper. Such processing is allowed if the controller conforms to Article 28 of the European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU).
- Multiple parties determine the purposes and means of the processing (GDPR, Regulation 2016/679/EU, Article 26, European Parliament and Council, 2016).
  - The electricity market comprises several entities like energy suppliers, distributors, and retail sellers. Multiple parties need some data. For example, both the distributor and the retail seller need the billing value. Consequently, one of the entities typically performs the readout and shares the metered value with the other party.
  - Recall that the European Commission Recommendation of March 9, 2012 (European Commission, 2012) on preparations for the roll-out of smart metering systems (2012/148/EU) calls for a clear determination of the responsibilities of data controllers and data processors. CJEU

recently decided on several cases concerning issues in controllership (see C-210/16, CJEU, 2018a; C-25/17, CJEU, 2018b; and C-40/17, CJEU, 2019b). For example, Advocate General Mengozzi (2018, paragraph 68) considers it necessary to rely upon a factual rather than a formal analysis. The European Parliament (2021) Resolution of March 25, 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation 2 years after its application (GDPR, 2020/2717(RSP), European Parliament, 2021) explicitly mentions ICT manufacturers being considered controllers of personal data.

◦ Polčák & Matoušek (2022) reported a case in which an association of coowners (condominium) deployed an AMR metering system with frequent readouts offered by a supplier. The association was interested in providing billing. However, the supplier installed a metering system that performs frequent readouts (with a period of tens of seconds). Who is the controller of the data in the frequent readouts, and who decides the purposes of the processing? Polčák & Matoušek (2022) only speculate about the accurate answer to this question. The supplier could have prevented the uncertainty by revealing the readout period. Consequently, the controller could have established that there is no legal basis for such transfers unless the inhabitants of each household give their free consent. Additionally, the parties should have signed a contract in conformance with European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU, Article 26). Such a contract arrangement would demonstrate adherence to the accountability principle.

Step 6: The controller should determine technical and organizational security measures (GDPR, Regulation 2016/679/EU, Article 32, European Parliament and Council, 2016). The controller should focus on the availability, integrity, confidentiality, authentication, identification of authorized personnel, nonrepudiation, access control, accountability, and auditing (GDPR, Regulation 2016/679/EU, European Parliament and Council, 2016; Kumar et al., 2019). A typical smart metering system is heterogeneous. The controller needs to identify the assets, responsibilities of the employees, threats, risks, and possible mitigations. Kumar et al. (2019) provide a thorough list of risks associated with metering networks of all sizes. Moreover, they identified solutions to some of the threats. Nevertheless, some of the identified threats are still open research problems. Known threats evolve, and the complexity of the deployed smart network often increases as new functionality is added and parts of the networks are replaced by new equipment. Hence, this step needs to be repeated, and the threats and risks revised. The controller should have a policy specifying the events that trigger the security reevaluation. The author of this chapter advises the controller to follow security standards like ISO/IEC 27000 that give holistic guidance on how to achieve secure deployment.

- Not only are the security measures essential for the data protection of the consumers, but they are also crucial for maintaining the stability of the metering systems. For example, Komninos et al. (2014) give an example of smart homes using parked electric cars' batteries to offer network energy during a high load. A man-in-the-middle attacker can massively drop the acknowledgment messages by the smart grid, resulting in unstable electricity network conditions.
- The system should be resilient against impersonation attacks (Komninos et al., 2014). An impersonating adversary can order the system to turn all devices on-premise on (with a financial burden on the customer) or off (with possibly life-threatening consequences if electrical life support systems are deployed).
- Asghar et al. (2017) mention tempered electric and gas meters in the United Kingdom, even though the tampering may result in explosions and even deaths. To overcome the issue, they recommend employing a scalable access control mechanism and application of low-level code of the smart meters.

Step 7: Once the controller completes the six steps above, they determine all crucial information to create records of processing activities (GDPR, Regulation 2016/679/EU, Article 30, European Parliament and Council, 2016). The records of processing activities enable the controller to prepare transparent information (GDPR, Regulation 2016/679/EU, Articles 12 and 13, European Parliament and Council, 2016). Cuijpers & Koops (2012) and Asghar et al. (2017) show that consumers need to be adequately informed about the risks and privacy implications of smart meters. Additionally, the controller should determine that there are means to allow data subjects to exercise the rights for data access (GDPR, Regulation 2016/679/EU, Article 15, European Parliament and Council, 2016), rectification (GDPR, Regulation 2016/679/EU, Article 16, European Parliament and Council, 2016), erasure (GDPR, Regulation 2016/679/EU, Article 17, European Parliament and Council, 2016), restriction of processing (GDPR, Regulation 2016/679/EU, Article 18, European Parliament and Council, 2016), and data portability (GDPR, Regulation 2016/679/EU, Article 20, European Parliament and Council, 2016).

- This step poses a risk for the controller. While data subjects should have means to exercise their rights, this process should not infringe on the rights of other data subjects. McKenna et al. (2012) raise the issue of multiple persons living in a single household. How can the controller distinguish between personal data belonging to a parent and an adolescent child, or distinguish between a landlord and a tenant? The author of this chapter suggests that the controller needs to evaluate each request on a case-by-case basis. The controller should prepare in advance for such requests and determine the process that determines if the request does not interfere with the rights of other individuals.

Step 8: As an additional step, the controller should increase the transparency of the processing. That is not strictly required by European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) but can be required by some national data protection laws. Additionally, as covered in Table 1, transparency can facilitate the deployment of smart metering. For example, the controller can allow the residents (data subjects) to read wireless data sent by the meters, offer access to the algorithms that analyze the metering data, or publish the data protection impact assessment or regular reports on the processing.

- The offer to read data demonstrates compliance with the rights for the data access (GDPR, Regulation 2016/679/EU, Article 15, European Parliament and Council, 2016) and data portability (GDPR, Regulation 2016/679/EU, Article 20, European Parliament and Council, 2016). For example, some residents do not want the controller to collect frequent readouts that are not necessary (Knyrim & Trieb, 2011). However, a resident wants to process the readouts themselves or forward them to an IoT vendor of the resident's choice. Such an option enables the customers to detect events such as water leakage as early as possible. Moreover, the customers could detect events tailored to a specific household (for example, the IoT controller can report any gas consumption when all household members are away as a gas leakage).
- The additional steps improve transparency (GDPR, Regulation 2016/679/EU, Articles 12 and 13, European Parliament and Council, 2016). The author of this chapter thinks that the more transparent the metering is, the less likely it encounters opposition. Moreover, transparency can improve the system's resiliency, and independent audits can improve the metering system. Data subjects that can validate the metering systems fear less compared to residents left in the dark about the data collected on their household.

Table 2 summarizes the steps and the European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU) principles affected during each step.

Table 2. Summary of the steps

Steps	Step summary
1. List processing operations	Transparency, purpose limitation, accountability
⇓	
2. Specify needed data	Fairness, transparency, purpose limitation, data minimization, accountability, data protection by design, risks for data subjects
⇕	
3. Legal basis for processing	Lawfulness, fairness, transparency, purpose limitation, necessity, accountability, legal bases, data protection by default, risks for data subjects, data protection impact assessment
⇕	
4. Storage duration	Lawfulness, fairness, transparency, data minimization, accountability, data protection by design and default, risks for data subjects, data protection impact assessment
⇓	
5. Identify other parties	Transparency, accountability
⇓	
6. Security measures	Accountability, risks for data subjects
⇓	
7. Records of processing and data subjects' rights	Lawfulness, fairness, transparency, purpose limitation, data minimization, accountability, legal bases, data protection by design and default, data subjects' rights
⇓	
8. Transparency and data access	Fairness, transparency, necessity, data subjects' rights

Note. The author of the chapter expects that the controller might iterate between steps 2–3 as they learn more details on the processing and risks for data subjects.

Manufacturers and Distributors of Components for Metering Systems

Recall that in the second and third steps, the entities running a metering system needed to perform a market analysis to identify meters with an adequate and preferably strictly necessary frequency of readouts and process only necessary information. A responsible manufacturer (or distributor) of remotely readable meters and other components for smart metering and smart grids should be transparent in documenting the capabilities and risks of the devices.

To facilitate the deployment of metering systems, the manufacturers and distributors should clearly explain the benefits of the meters. For example, they can educate on the risk of postmeter leakage, which accounts for up to 10% of total water consumption (Britton et al., 2013). Recall that the entity running the meter needs to justify the costs in proportion to the expected energy savings (Directive 2018/2002/EU, European Parliament and Council, 2018). A controller determining the purposes of processing (steps 1 and 2 above) can precisely justify the processing only if the manufacturers and distributors provide transparent and precise information.

The manufacturers should make the devices configurable. Some protocols like Wireless M-Bus (EN 13757) need frequent data transmissions. Polčák & Matoušek (2022) reported meters sending data with a period of tens of seconds or minutes. As some deployments (like billing) do not need such frequent readouts, the manufacturer should allow a household member to configure the frequency of the readouts. For example, it is technically possible to keep sending the same metered value for each transmission for a whole month. As faulty or tampered gas or electricity meters can cause explosions (Asghar, 2017), the manufacturers should consider allowing verification of the meters' firmware, for example, by an independent certification body.

A metering system can consist of a web interface, application, or a similar user interface facing the resident of a metered household. Such an interface can provide historical data on billing and consumption. Recall that the controller needs to decide on envisaged time limits for the erasure of the collected personal data (step 4 above, GDPR, Regulation 2016/679/EU, Article 5(1)(e), European Parliament and Council, 2016). Hence, the web interface and the underlying database need to erase data after the period during which the controller needs the data. The vendor should allow the user to consent to keep data longer than necessary.

The manufacturer and the distributor should clearly describe the security model and support. For example, is the security strong enough to protect confidentiality, integrity, availability, authenticity, and other security functions? What are the privacy goals (Kumar et al., 2019)? Will there be software updates for the device? Are there any known attacks against the devices? Is it possible to pay for security support, or is it included in the price of the meter? What is the envisioned threat model?

The manufacturer should incorporate the possibility of using encrypted personal data and cryptographic proofs (Rial et al., 2018) or homomorphic encryption. As mentioned above, such an approach demonstrates legal conformance, does not leak private data to energy distributors, and does not need excessive additional resources. If such approaches are not applicable, the manufacturer should enable the meter to compute some operations like fraud detection directly in the meter so that the consumption data do not need to be processed and collected by other elements of the metering architecture.

Some of the above recommendations are motivated by business incentives. The author of this paper believes that a meter detecting events like meter tampering or water leakage should sell better than a meter without such configurability. However, the manufacturers and distributors must also be motivated by the data protection law.

The European Parliament (2021) Resolution of March 25, 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation 2 years after its application (GDPR, 2020/2717(RSP), European Parliament, 2021), explicitly considers ICT manufacturers as controllers according to Article 4(7) (GDPR, Regulation 2016/679/EU, European Parliament and Council, 2016), as they determine the means of processing. Although such a statement is not lawfully binding, the manufacturers (and distributors) should be aware of the possibility of them being a controller. The author of this text believes that manufacturers and distributors should avoid any possibility of them being identified as actual controllers (if they do not have a business model depending on them being a controller). Controllers have many legal requirements that can be avoided by the manufacturers by offering sufficient transparency to the actual controllers.

Considered Scenarios

This section applies the data protection recommendation to metering systems (scenarios) and clarifies the views of the author of this chapter.

Scenario A: Manual Water Remote Readout

This scenario deals with a building, that is, owned by an association of co-owners or a condominium. The building is composed of many units. Each building unit has a water meter that can be read remotely. However, there is no additional permanent infrastructure. Such a metering system is cost effective, as it does not require permanent reading, and the electricity consumption is minimal. However, a person needs to enter the building or read the data in front of the building, as the signal strength is sufficient for readouts from the vicinity only. The controller is the association of co-owners. However, as it is a small entity without any knowledge of security in information technologies, it will need help to manifest conformance with the law.

Step 1: The controller decides that it needs to process data to provide billing. Additionally, the controller is interested in detecting events (Polčák & Matoušek, 2022). Although the metering system cannot warn about accidents in real time, as there is no reading infrastructure, the meters can detect tampering, backflow, and similar events (Polčák & Matoušek, 2022).

Step 2: The controller determines that it needs monthly data readouts to comply with Directive 2018/2002/EU (European Parliament and Council, 2018). For each detectable event, the controller only needs information if the event was or was not detected during the previous month.

Step 3: The controller decides to process billing information as a legal obligation. The controller will process events as its legitimate interests, as it will process only strictly necessary information to prevent fraud and ensure proper billing.

Step 4: The controller will keep personal data for the period required by law. For personal data that are not required by law, like the detected events, the controller can store such personal data for the duration of the investigation that explains and settles the event.

Step 5: The controller does not plan to buy a reading set. It will buy a specialized service to perform the reading.

Step 6: The controller will ensure organizational and security measures as a service offered by the manufacturer of the meter.

Steps 7–8: These steps do not add any technical steps and are out of the scope of this chapter.

The manufacturer of the meters has to help the controller. The manufacturer does not want to be considered a controller, so it discloses all information regarding data transfers to the controller. This should include any quirks of the protocol, such as the necessity to transfer data much more often than needed, as explained in the case of a Wireless M-Bus described in a deployment by Polčák & Matoušek (2022). The manufacturer takes several steps to account for the compliance of deployed meters with the law. Although the meters send data every minute, all messages contain the same readout from the beginning of the month. The meters keep several recent readings in local memory to detect the events. To increase transparency and facilitate the expansion of the systems, the manufacturer gives the controller instructions on how to read the messages and switch the meters to more frequent readouts. Tenants in the building can buy their own reading sets to track their consumption. The manufacturer also offers a paid service (that gives it additional revenue) that tracks all changes in related standards, data protection laws, and published security threats. The service will warn the controller in case there is any problem. The meters can be updated to fix bugs or be updated according to new requirements.

Scenario B: Manual Gas Remote Readout

In this scenario, a gas distributor (controller) installs meters to building units. The meters send data wirelessly and are not connected to any permanent infrastructure. Similarly to scenario A, a car needs to park in front of the building to read out the metering data. The signal strength is sufficient for readouts from the vicinity only.

Steps 1–4: The motivations of the controller are the same as in Scenario A (see the concrete steps above).

Step 5: The controller will perform the reading by itself. However, the controller decides to store the readouts in the cloud. The controller needs to ensure that all provisions that are out of the scope of this paper are met (European Data Protection Board, 2021; C-311/18, CJEU, 2020).

Step 6: The controller is large enough to organize the security by itself. Nevertheless, it will cooperate with the manufacturer of the meters and react to any vulnerability found. Additionally, it will review related work biannually to consider new risks for the processing.

Steps 7–8: These steps do not add any technical steps and are out of the scope of this chapter.

Similarly, to Scenarios A and B, there are many variants that influence the outcome of the analysis only slightly.

Scenario C: Permanent Infrastructure—Frequent Readouts

In this scenario, a gas distributor (controller) installs meters to building units in a small city. The meters send data wirelessly to a radio station mounted on the building of the distributor in the city. The signal strength is sufficient for the readouts.

Step 1: The controller decides that it needs to process data to provide billing. Additionally, the controller is interested in detecting events like meter tampering or backflow. The metering system will warn about accidents in real time.

Step 2: The controller determines that it needs monthly data readouts to comply with Directive 2018/2002/EU (European Parliament and Council, 2018). The controller does not find any meter on the market that detects all required events, so it will need frequent readouts.

Step 3: The controller decides to process billing information as a legal obligation. The controller will process events as its legitimate interests. However, as the amount of data required is high, it will consult with its data protection authority (GDPR, Regulation 2016/679/EU, Articles 35 and 36, European Parliament and Council, 2016). The controller and the supervisory data protection authority decide to apply additional safeguards including public reports, incentives to review the algorithms, or the possibility of opt-out. The controller might be ordered to postpone the processing and run a pilot study with volunteers. If the controller is large enough, it might conduct a business contract with a manufacturer to deliver meters suitable for the task. The controller can deploy meters detecting fraud and leakage in suitable locations like where the flow is aggregated.

Step 4: The controller will keep personal data for the period required by law. For personal data that are not required by law, like the readouts to detected events, the controller will immediately delete the data unless it detects an event. The controller will store personal data that triggered the event for the duration of the investigation that explains and settles the event.

Steps 5–8: See the scenarios above.

Scenario D: Permanent Infrastructure—Optional Processing Based on Consent

This scenario is similar to Scenario A. However, the controller decides to deploy a permanent reading infrastructure. The infrastructure consists of gateways that forward the readouts through the internet to a server collecting and processing the data. The advantage for the association is that the billing is performed automatically. All tenants have access to the metered data in real time. Moreover, the deployment can detect water leaks. The association decides that preventing the risk of a water leak and giving the possibility to the tenants to track and optimize the consumption outweigh the cost of the reading infrastructure.

The steps needed to be taken by the controller are very similar to Scenario A. Table 3 introduces the new processing activities. Step 4 is similar to Scenario A.

Table 3. Additional processing of the controller

Step 1	Step 2	Step 3
Water leak detection	Event detected by meter	Legitimate interests, see the reasoning for similar processing in Scenario A
Detailed information on water consumption	Detailed data like the consumption at the time of each message from the meter	Consent of the tenants. The meter needs to be switched manually.

Note. Each line represents one processing activity.

The service provider will offer a paid service that enables the controller to allow the tenants to see the detailed consumption. As detailed consumption tracking is not strictly necessary, the controller cannot force all tenants to allow the processing. As a result, such data will be collected only with freely given consent. Some tenants will participate, and others will not.

Scenario E: Detection of Unlawful Water Consumption During Drought

In this scenario, a local water distributor installs meters to building units and households in a city. The meters send data wirelessly to radio stations mounted on communal buildings in the city. The signal strength is sufficient for the readouts. In essence, this scenario is similar to Scenario C. However, in this case, local authorities ask the distributor to give them data on unusual patterns in consumption that might reveal temporarily banned activities like filling pools.

In this case, there are two controllers. The water distributor deployed the metering system similar to the discussion in Scenario C. The local authorities are a different controller (C-175/20, 2022, CJEU,2022). Hence, the local authorities need to go through the identified steps by themselves:

Step 1: Personal data are needed to identify illegal water usage.

Step 2: The local authorities can ask for: (1) detailed readings, (2) identified events, and (3) running algorithms on the data in possession of the local water distributor. In all three cases, the local distributor is the processor that acts on behalf of the local authorities.

Step 3: The local authorities decide that the processing is necessary for the performance of a task carried out in the public interest (GDPR, Regulation 2016/679/EU, Article 6(e), European Parliament and Council, 2016). However, unless there is a law following Article 23, European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU), the processing cannot be carried out.

Step 4: The law identified in step 3 will likely specify the period for how long the local authorities keep the data or how the period should be calculated. Otherwise, local authorities should immediately delete personal data for households without suspicion. The local authorities will keep suspicious data during the investigation of the incident or for the time required by the law governing the investigations.

Step 5: Both the water distributor and local authorities are controllers. The water distributor is a processor of local authorities. Depending on additional circumstances out of the scope of this chapter, there might be additional processors.

Step 6: Both parties need to negotiate the security measures to transfer personal data with regard to the sensitivity of the data.

Step 7: The local authorities need to prepare the records of processing activities and are responsible to obey user rights.

Scenario F: Undocumented Data Transmitted by the Meters

A controller deployed a metering system similar to the Scenarios A–D. The controller fulfilled all its responsibilities and deployed the system. The police investigate a burglary in one of the households and learn that the burglars used data transmitted wirelessly by the metering systems to reveal occupancy periods of the household. The police forward the case of the metering system to the data protection authority. The controller demonstrates that it deployed meters that were supposed to provide monthly readouts with Directive 2018/2002/EU (European Parliament and Council, 2018), and the documentation does not mention more frequent readouts. The supervisory authority fines the manufacturer of the meters and orders replacing the meters.

The manufacturer did not follow the advice given in this chapter and was not transparent. As a consequence, it was the manufacturer that decided that frequent data are collected on data subjects. However, such processing was not lawful, as it was not collected for legitimate purposes in a transparent manner.

Scenario G: Security Breach

An adversary managed to get access to the database collected in Scenario D. A data subject sues the controller for the data breach. As the controller followed the steps listed in this chapter, it can demonstrate that all personal data were processed lawfully, fairly, and in a transparent manner. As the controller can demonstrate a legal basis for storing all leaked data in the database, and it was able to demonstrate that all security measures were in place as required by Article 32 of European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU), the lawsuit is dismissed.

For example, the Supreme Administrative Court of the Czech Republic recently stated that a controller could not be held responsible for any security breach, and the data protection authority needs to demonstrate that the level of security was not appropriate to the risk of a breach (Supreme Administrative Court of the Czech Republic, 2021).

Scenario H: Electrical Energy Grid

Knapp & Samani (2013) give an overview of an electrical grid. There are producers of energy like fossil, nuclear, solar, hydroelectric, and wind power plants. The electricity is carried by the transmission and distribution layer. At this stage, the electricity is carried by high-voltage transmission. Transformers can increase (step up) or decrease (step down) voltages. Households are connected to the distribution network, each having a meter. A household can generate electricity, for example, with a solar panel. A household can also utilize devices that communicate with the network, for example, to negotiate the best time to consume energy.

Several entities play a role in the architecture. Energy producers need to know and predict how much energy to produce. Transmission entities need to prevent the network from blackout. They need to balance the amount of energy accepted for the transmission with the consumed energy. They also need models for anticipating the imminent behavior of the network. They also need data to perform billing. Distribution network operators need data to perform billing. Households need means to communicate with other parties to negotiate energy consumption and price. Note that such deployments facilitate complex pricing schemes. Energy can be ordered in advance but also bought at the last moment. As a result, many personal data controllers appear—producers, transmission, and distributors need to process personal data. Table 4 contains processing activities, needed data, and possible legal basis for such operation. Note that it is out of the scope of this chapter to provide an exhaustive list of processing activities in the smart grid. The listed processing activities are examples of activities that can be performed.

Table 4. An example of processing activities in a smart electrical grid

Entity	Step 1	Step 2	Step 3	Step 5
Producer	Price negotiation	Negotiated price, consumption period, energy sold, and energy consumed	Performance of a contract	(Some) data shared with transmission and distribution
Transmission	Billing	Aggregated data for the billing period. Dynamical contracts accepted by producers.	Performance of a contract	
Distribution	Billing	Aggregated data for the billing period. Dynamical contracts accepted by producers.	Performance of a contract	
Distribution	Fraud prevention	Aggregated data, in case of suspicion, detailed data	Legitimate interests, steps taken so that the interests of the controller are not overridden by the interests of the data subject	(Some) data shared with distribution, law enforcement, etc.
Producer, transmission, distribution	Predict future load	Aggregated data collected by transformers	Personal data are not processed, so these steps do not apply.	

Note. Each line represents one processing activity.

Of course, this scenario can be expanded. The amount of personal data will depend on the specific parameters of each deployment. The purpose of this example is to illustrate that aggregated data greatly simplify the obligations of data controllers. The key question is how to get the aggregated data. As Recommendation 2012/148/EU (European Commission, 2012) and European Parliament (2021) Resolution 2021/C494/11 suggest, the best time to answer the question is before the deployment. The earlier the processing activities are detected, the lower the time to design or redesign the grid.

GENERALIZATION OF THE RECOMMENDATIONS FOR SMART HOMES

The European Commission (2014) (Recommendation 2014/724/EU) on the data protection impact assessment highlights that data from smart grids can be combined with other sources, such as geolocation data, tracking and profiling on the internet, video surveillance systems, and radio frequency identification (RFID) systems. According to the Recommendation, Article 29 Working Party and Commission

(2014) see smart metering as a foreshadowing of the IoT. This section reiterates the steps suggested above in the context of IoT deployment.

Devices typically appearing in smart homes, like smart bulbs, smart thermostats, smart plant watering, or smart ovens, produce and process personal data. Such devices often propagate data to the servers of the manufacturer or service provider (e.g., running in the cloud). According to European Parliament and Council (2016) (GDPR, Regulation 2016/679/EU), these service providers are data controllers.

Consequently, the controllers need to:

- track the operations (step 1 above),
- determine data needed to achieve the goal, including data minimization and necessity (step 2),
- decide the lawfulness of the processing (step 3),
- decide the envisaged time limits (step 4),
- reflect other parties (step 5),
- determine technical and organizational security measures (step 6),
- create the records of processing, and check that there are means to exercise the rights (step 7).

The author of this text thinks that step 8 typically does not make sense for IoT deployments. The difference is that in smart metering, the consumers typically cannot decide that they do not want the metering. In IoT, the customer decides to engage in a business contract with the controller. Step 8 is optional and aims to facilitate smart metering deployment.

FUTURE RESEARCH DIRECTIONS

The author of this chapter agrees with Orlando & Vandelvelde (2021) that current guidelines for smart metering lack clear guidance on the aggregation of data. Recall California, New York, and the rule that specifies the minimal number of households and maximal share of consumption of each household. Such numbers are understandable and implementable. Nevertheless, such a rule does not exist in Europe. According to Article 29 Data Protection Working Party (2014) Opinion 05/2014 on anonymization techniques, every case needs to be considered independently. Nevertheless, a branch of future research can focus on testing the rules of California, New York, or similar rules. Can such a rule guarantee that the aggregated data cannot be reversed? If not, do we need to add additional households, lower the maximal consumption, or add other constraints like spreading the consumption into small time bins?

This chapter identified multiple scenarios. However, there are likely other scenarios. Are there other requirements for these scenarios? Moreover, the chapter generalized the findings to smart homes. However, IoT also covers deployments that do not process personal data. One future research direction can focus on various flavors of IoT and the need for personal data.

From the law's point of view, the roles of the parties can be blurred. Possible research can focus on identifying the roles of each party. Who needs to be a controller, and who may be considered only a processor?

Another open question is the minimal subset of functionality and configurability of a meter. Cuijpers & Koops (2012) describe the failed attempt at smart meter roll-out in the Netherlands. One of the obstacles to the roll-out was that the meters were planned to be controllable remotely. Hence, identifying a minimal set of functionalities can help with legal certainty as well as in courts.

Kumar et al. (2019) cover the open security issues well (GDPR, Regulation 2016/679/EU, Article 32, European Parliament and Council, 2016). According to their paper, most of the research is evaluated by simulation instead of real-world devices. Only a few researchers evaluate their security properties with real smart meters, probably due to the limited access to real-world devices. Another issue lies in applying homomorphic and advanced cryptography to meters that need to conserve power. Advanced key distribution schemes are an open issue, as current schemes are vulnerable or have high computational costs. The limited communication bandwidth in metering networks results in the need to design secure and efficient routing protocols. Wireless transfers are inherently vulnerable to jamming and spoofing attacks. Another open research question, according to the paper, is the need for detailed data. Finally, they identified the need for security and privacy assessment tools.

Additionally, open research questions concern the practical large-scale deployment of homomorphic encryption smart meters or smart meters using cryptographic proofs (Rial et al., 2018) in multiple EU member states. The research should focus on facilitating such deployments. What are the benefits for manufacturers and utilities? Can the benefits be made more significant?

CONCLUSION

Our lifestyles depend on functioning utilities. It is well understood that energy consumption can be reduced by eliminating waste. The improvements in leakage detection can save up to 10% of the water (Britton et al., 2013). Fraud and energy theft harm the utilities. Smart metering provides the possibility to improve energy consumption. However, the deployment of smart networks brings several challenges to the design and operation of critical infrastructure. The network or individuals can be targeted, and, for example, an attack can stop energy distribution and harm individuals or companies (Kumar et al., 2019). It is well understood that a secure system needs to be designed securely from the beginning (Kumar et al., 2019). This chapter provides an overview of the metering networks, known threats, and the literature. The main contribution lies in specifying detailed steps that achieve conformance with data protection laws. A metering system designed according to the steps outlined in this chapter is resilient to threats and processes only necessary personal data. The chapter illustrates the application of scenarios and the steps ranging from a small deployment to a full-scale grid. The requirements apply to any energy distribution system, provided that the system meters the consumption of individual persons and, in some countries, small groups of persons. Moreover, the author argues that the steps can help smart home device manufacturers in designing data protection-compliant devices and services.

REFERENCES

Abreu, Z., & Pereira, L. (2022). Privacy protection in smart meters using homomorphic encryption: An overview. *WIREs*, *12*(4), 1–16. doi:10.1002/widm.1469

Armel, K., Gupta, A., Shrimali, G., & Albert, A. (2013). Is disaggregation the holy grail of energy efficiency? The case of electricity. *Energy Policy*, *52*(1), 213–234. doi:10.1016/j.enpol.2012.08.062

Asghar, M. R., Dán, G., Miorandi, D., & Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communications Surveys and Tutorials*, *19*(4), 2820–2835. doi:10.1109/COMST.2017.2720195

Backes, M., & Melser, S. (2012). Differentially private smart metering with battery recharging. *IACR Cryptology*, 183. https://eprint.iacr.org/2012/183

Beal, C. D., & Flynn, J. (2015). Toward the digital water age: Survey and case studies of Australian water utility smart-metering programs. *Utilities Policy*, *32*, 2–37. doi:10.1016/j.jup.2014.12.006

Britton, T. C., Stewart, R. A., & O’Halloran, K. R. (2013). Smart metering: Enabler for rapid and effective post meter leakage identification and water loss management. *Journal of Cleaner Production*, *54*, 166–176. doi:10.1016/j.jclepro.2013.05.018

Brunschwiler, C. (2013). *Wireless M-Bus security*. Black Hat.

California Public Utilities Commission. (2014). *Decision adopting rules to provide access to energy usage and usage-related data while protecting privacy of personal data*. CPUC. https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M090/K845/90845985.PDF

Chen, D., Irwin, D., Shenoy, P., & Albrecht, J. (2014). *Combined heat and privacy: Preventing occupancy detection from smart meters*. In *2014 IEEE International Conference on Pervasive Computing and Communications*, (pp. 208–215). IEEE.

Chen, F., Dai, J., Wang, B., Sahu, S., Naphade, M., & Lu, C.-T. (2011). *Activity analysis based on low sample rate smart meters*. In *Proceedings of the 17th ACM International Conference on Knowledge Discovery and Data Mining*, (pp. 240–248). ACM. 10.1145/2020408.2020450

Court of Justice of the European Union. (2010). *Joint Case C-92/09 and C-93/09 (2010). Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*. [*Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*.] Europea. https://curia.europa.eu/juris/liste.jsf?num=C-92/09

Court of Justice of the European Union. (2013). *Case C-473/12. Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others*. [*Professional Institute of Realtors (IPI) v Geoffrey Englebert and Others*.]. Europa. https://curia.europa.eu/juris/liste.jsf?num=C-473/12

Court of Justice of the European Union. (2014). Case C-212/13. *František Ryneš v Úřad pro ochranu osobních údajů.* [*František Ryneš in the Office for Personal Data Protection.*] Europa. https://curia.europa.eu/juris/liste.jsf?num=C-212/13

Court of Justice of the European Union. (2016). Case C-582/14. *Patrick Breyer v. Bundesrepublik Deutschland.* Europea. https://curia.europa.eu/juris/liste.jsf?num=C-582/14

Court of Justice of the European Union. (2017). Case C-13/16. *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA "Rīgas satiksme"*. [*Order Police Department of the Riga Region Administration of the State Police v. Riga Municipality Ltd. "Rīgas* satiksme".]. Europea. https://curia.europa.eu/juris/liste.jsf?num=C-13/16

Court of Justice of the European Union. (2018a). Case C-210/16. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*. [*Unabhängiger Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*.]. Europa. https://curia.europa.eu/juris/liste.jsf?num=C-210/16

Court of Justice of the European Union. (2018b). Case C-25/17. *Jehovah witness.* Europa. *https://curia.europa.eu/juris/liste.jsf?num=C-25/17*

Court of Justice of the European Union. (2019a). Case C-708/18. *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*. [*TK v. Association of Owners block M5A-ScaraA*.]. Europa. https://curia.europa.eu/juris/liste.jsf?num=C-708/18

Court of Justice of the European Union. (2019b). Case C-40/17. *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV.* https://curia.europa.eu/juris/liste.jsf?num=C- 40/17

Court of Justice of the European Union. (2020). Case C-311/18. *Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems.* Europa. https://curia.europa.eu/juris/liste.jsf?num=C- 311/18

Court of Justice of the European Union. (2022). Case C-175/20. *„SS" SIA v. Valsts ieņēmumu dienests*. [*"SS" Ltd. v. State Revenue Service*.] https://curia.europa.eu/juris/liste.jsf?num=C- 175/20

Cuijpers, C., & Koops, B.-J. (2008). The 'smart meters' bill: A privacy test based on article 8 of the ECHR. *Study commissioned by the Dutch Consumers' Association*. English version available from the authors, see Cuijpers, C., & Koops, B.-J. (2012), footnote 39.

Cuijpers, C., & Koops, B.-J. (2012). Smart metering and privacy in Europe: Lessons from the Dutch case. In *European data protection: Coming of age* (pp. 269–293). Springer.

Erol-Kantarci, M., & Mouftah, H. T. (2013). Smart grid forensic science: Applications, challenges, and open issues. *IEEE Communications Magazine*, *51*(1), 68–74. doi:10.1109/MCOM.2013.6400441

Esposito, C., & Ciampi, M. (2015). On security in publish/subscribe services: A survey. *IEEE Communications Surveys and Tutorials*, *17*(2), 966–997. doi:10.1109/COMST.2014.2364616

European Commission. (2011). Programming Mandate M/487 EN. *Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards*. European Commission. https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=472

European Commission. (2012). Recommendation 2012/148/EU. *Commission Recommendation of 9 March 2012 on preparations for the roll-outroll-out of smart metering systems. Official Journal of the European Union, L*, *73*(9), 9–22.

European Commission. (2014). Recommendation 2014/724/EU. *Commission Recommendation of 10 October 2014 on the data protection impact assessment template for smart grid and smart metering systems. Official Journal of the European Union, L, 300*(63), 63–68.

European Commission. (2011). Article 29 Data Protection Working Party. *Opinion 12/2011 on smart metering*. Europea. https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2011/wp183_en.pdf

European Commission. (2013). Article 29 Data Protection Working Party. *Opinion 05/2013 on purpose limitation*. Europea. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

European Commission. (2014). Article 29 Data Protection Working Party. *Opinion 05/2014 on anonymization techniques*. Europea. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

European Data Protection Board. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0.* Europa. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

European Parliament. (2021) *European Parliament Resolution 2021/C 494/11. European Parliament Resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)). European Parliament. Official Journal of the European Union* C 494/129-138.

European Parliament and Council. (2016). *General Data Protection Regulation (GDPR). Regulation 2016/679/EU. Official Journal of the European Union* L 119, 4.5.2016, 1–88.

European Parliament and Council. (2018). Directive 2018/2002/EU. *Amending Directive 2012/27/EU on energy efficiency. European Parliament and Council. Official Journal of the European Union* L 328, 21.12.2018, p. 210–230.

European Parliament and Council. (2019). Directive 2019/944/EU. *On common rules for the internal market for electricity and amending Directive 2012/27/EU.* European Parliament and Council. Official Journal of the European Union L *158, 14.6.2019, 125–199.*

Kaatz, J. (2017). Resolving the conflict between new and old: A comparison of New York, California and other state DER proceedings. *The Electricity Journal*, *30*(9), 6–13. doi:10.1016/j.tej.2017.10.005

Kalogridis, G., Efthymiou, C., Denic, S., Lewis, T., & Cepeda, R. (2010). Privacy for smart meters: towards undetectable appliance load signatures. In *2010 First IEEE International Conference on Smart Grid Communications*, 232–237. 10.1109/SMARTGRID.2010.5622047

Kelly, J., & Knottenbelt, W. (2015). The UK-DALE dataset, domestic appliance-level electricity demand and whole-house demand from five UK homes. *Scientific Data*, *2*(1), 1–14. doi:10.1038data.2015.7 PMID:25984347

Knapp, E. D., & Samani, R. (2013). *Applied cyber security and the smart grid*. Elsevier Inc.

Knyrim, R., & Trieb, G. (2011). Smart metering under EU data protection law. *International Data Privacy Law*, *1*(2), 121–128. doi:10.1093/idpl/ipr004

Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys and Tutorials*, *16*(4), 1933–1954. doi:10.1109/COMST.2014.2320093

Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J. S., & Martin, A. (2019). Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Communications Surveys and Tutorials*, *21*(3), 2886–2927. doi:10.1109/COMST.2019.2899354

Lee, D., & Hess, D. J. (2021). Data privacy and residential smart meters: Comparative analysis and harmonization potential. *Utilities Policy*, *70*, 101188. doi:10.1016/j.jup.2021.101188

Lima, C. A. F., & Navas, J. R. F. (2012). Smart metering and systems to support a conscious use of water and electricity. *Energy*, *45*(1), 528–540. doi:10.1016/j.energy.2012.02.033

Lisovich, M. A., Mulligan, D. K., & Wicker, S. B. (2010). Inferring personal information from demand-response systems. *IEEE Security and Privacy*, *8*(1), 11–20. doi:10.1109/MSP.2010.40

Liu, A., Giurco, D., & Mukheibir, P. (2015). Motivating metrics for household water-use feedback. *Resources, Conservation and Recycling*, *103*, 29–46. doi:10.1016/j.resconrec.2015.05.008

March, H., Morote, Á.-F., Rico, A.-M., & Saurí, D. (2017). Household smart water metering in Spain: Insights from the experience of remote meter reading in Alicante. *Sustainability*, *9*(4), 582. doi:10.3390u9040582

McKenna, E., Richardson, I., & Thomson, M. (2012). Smart meter data: Balancing consumer privacy concerns with legitimate applications. *Energy Policy*, *41*, 807–814. doi:10.1016/j.enpol.2011.11.049

McLaughlin, S., McDaniel, P., & Aiello, W. (2011). Protecting consumer privacy from electric load monitoring. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, (pp. 87–98). ACM. 10.1145/2046707.2046720

Mengozzi, P. (2018). Opinion of Advocate General Mengozzi. *CJEU Case C-25/17, ECLI:EU:C:2018:57.* https://curia.europa.eu/juris/liste.jsf?num=C-25/17

Mohassel, R. R., Fung, A., Mohammadi, F., & Raahemifar, K. (2014). A survey on advanced metering infrastructure. *Electrical Power and Energy Systems*, *63*, 473–484. doi:10.1016/j.ijepes.2014.06.025

Monedero, I., Biscarri, F., Guerrero, J. I., Roldán, M., & León, C. (2015). An approach to detection of tampering in water meters. *Procedia Computer Science*, *60*, 413–421. doi:10.1016/j.procs.2015.08.157

New York State Public Service Commission. (2018). *Order Adopting Whole Building Energy Data Aggregation Standard*. NYPSC.https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B4C4CE28E-54CC-4514-967D-B513678E3F37%7D

Orlando, D., & Vandelvelde, W. (2021). Smart meters' roll out, solutions in favour of a trust enhancing law in the EU. *Journal of Law. Technology & Trust*, *2*(1). Advance online publication. doi:10.19164/jltt.v2i1.1071

Polčák, L., & Matoušek, P. (2022). *Metering homes: do energy efficiency and privacy need to be in conflict*? In *Proceedings of the 19th International Conference on Security and Cryptography*, Lisboa, Portugal. 10.5220/0011139000003283

Rial, A., Danezis, G., & Kohlweiss, M. (2018). Privacy-preserving smart metering revisited. *International Journal of Information Security*, *17*(1), 1–31. doi:10.100710207-016-0355-8

Supreme Administrative Court of the Czech Republic. (2021). *Internet Mall, a.s. v. Úřad pro ochranu osobních údajů [Internet Mall, a.s. Office for Personal Data Protection].* SACCR. https://www.nssoud.cz/files/SOUDNI_VYKON/2021/0238_1As__2100033S_20211111111159.pdf

United States Court of Appeals for the Seventh Circuit. (2018). *Naperville Smart Meter Association v. Naperville - Seventh Circuit Decision.* United States Court of Appeals for the Seventh Circuit.

Yang, W., Li, N., Qi, Y., Qardaji, W., McLaughlin, S., & McDaniel, P. (2012). *Minimizing private data disclosures in the smart grid*. In ACM Conference on Computer and Communications Security, Raleigh, North Carolina. 10.1145/2382196.2382242

Zeifman, M., & Roth, K. (2011). Nonintrusive appliance load monitoring: Review and outlook. *IEEE Transactions on Consumer Electronics*, *57*(1), 76–84. doi:10.1109/TCE.2011.5735484

Zhou, S., & Brown, M. A. (2016). Smart meter deployment in Europe: A comparative case study on the impact of national policy schemes. *Journal of Cleaner Production*, *144*, 22–32. doi:10.1016/j.jclepro.2016.12.031

ADDITIONAL READING

Article 29 Data Protection Working Party (2014*). Opinion 8/2014 on Recent Developments on the Internet of Things.* Europa. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Edwards, L. (2016). Privacy, security and data protection in smart cities: A critical eu law perspective. *European Data Protection Law Review*, *2*(1), 28–58. doi:10.21552/EDPL/2016/1/6

European Court of Human Rights. (2022). *Guide on Article 8 of the European Convention on Human Rights.* ECHR. https://www.echr.coe.int/documents/guide_art_8_eng.pdf

European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0.* EDPB. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

European Data Protection Board. (2021). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.1*. EDPB. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Finster, S., & Baumgart, I. (2015). Privacy-aware smart metering: A survey. *IEEE Communications Surveys and Tutorials*, *17*(2), 1088–1101. doi:10.1109/COMST.2015.2425958

Jakobi, T., Patil, S., Randall, D., Stevens, G., & Wulf, V. (2019). It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Transactions on Computer-Human Interaction*, *26*(1), 1–44. doi:10.1145/3281444

Langås, M., Løfqvist, S., Katt, B., Haugan, T., & Jaatun, M. G. (2021). *With a little help from your friends: Collaboration with vendors during smart grid incident response exercises. European Interdisciplinary Cybersecurity Conference (EICC)*. Association for Computing Machinery, New York, NY, USA, 46–53. 10.1145/3487405.3487654

Petrlic, R. (2019). The General Data Protection Regulation: From a data protection authority's (technical) perspective. *IEEE Security and Privacy*, *17*(6), 31–36. doi:10.1109/MSEC.2019.2935701

Singh, J., & Cobbe, J. (2019). The security implications of data subject rights. *IEEE Security and Privacy*, *17*(6), 21–30. doi:10.1109/MSEC.2019.2914614

KEY TERMS AND DEFINITIONS

Advanced metering infrastructure (AMI): This is heterogeneous and hierarchical; it includes smart meters, communication networks, data management systems, and means to integrate collected data into software platforms and interfaces. AMI allows bidirectional communication, typically initiated by the infrastructure. Typical AMI meters allow advanced features to improve the reliability, efficiency, and sustainability of the grid. For example, connected devices can negotiate with the network the optimal time to consume resources (for example, to charge an electric vehicle during the night).

Automatic metering readout (AMR): This allows only communication initiated by the meters and often without the possibility of sending data to the meter. The meters are typically not directly connected to a wired network and are powered by batteries. The goal is to minimize the power requirements of the meter. The meters are typically read by a person that enters the building or parks a car in the vicinity. There might be a permanent infrastructure to read the meters.

Court of Justice of the European Union (CJEU): This is the highest court in the European Union. Courts in the European Union should take into account its case law.

Controller: This is an entity defined by GDPR that specifies the means and purposes of the processing of personal data.

Personal data: These are any data that can be directly or indirectly connected to a natural person, for example, by using identifiers.

Privacy: This is a concept that allows a person to keep information hidden from the general public. It is connected to the right to respect for private and family life in the European Convention of Human Rights and respect for private and family life, protection of personal data of the European Charter of Fundamental Rights.

Processor: This is an entity cooperation with the controller processing personal data according to the instructions of the controller.

Smart meter: This is a device with capabilities like remote readout, remote control, price negotiation, etc. A typical smart meter does not offer all capabilities.