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 where 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 networks legally compliant. Additionally, the chapter lists recommendations for smart meter manufacturers that removes the burden of being a controller of the processing. The chapter shows that the recommendations can be generalized for smart home deployments.

Keywords: Smart Metering, Privacy, GDPR, Data Protection, Legal Compliance, Energy Efficiency, Personal Data, Wireless M-Bus, Controller, Processor

INTRODUCTION

The European Union 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, 2015) and water leakage (Britton et 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 2018/2002/EU, Article 9b(1) and 9c).

The EU Directive on common rules for the internal electricity market provides requirements for smart metering systems (Directive 2019/944/EU, Article 20). 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)). "*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)). Nevertheless, the deployment of smart metering for electricity metering is not mandatory and should be decided by each EU member state by an assessment (Directive 2019/944/EU, Article 19(2)).

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). A poorly designed metering systems risk incompatibilities with data protection laws (Polčák & Matoušek, 2022). Consequently, utilities deploying such a system risks a ban from competent authorities

or an order to redesign the system. Such risks 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 what is technically feasible for remotely readable monitoring systems. In particular, the text of the chapter argues that data processed by the metering systems are often personal data and the EU General Data Protection Regulation 2016/679/EU (GDPR, 2016) typically applies. Consequently, the requirements of GDPR (Regulation 2016/679/EU) on controllership, data minimization, transparency, and fairness must be fulfilled. Moreover, the chapter provides suggestions on how to architect and deploy metering systems that fully conform to law requirements. To facilitate the understanding, the chapter introduces three scenarios of possible smart metering networks, ranging from a small network to a full electricity smart grid. Finally, the chapter generalizes the requirements for smart homes.

Cuijpers & Koops (2012) describe the failure of smart metering deployment in the Netherlands. The deployment failed due to detail readouts; processed data were not supposed to be minimized and necessary. The main goal of this chapter is to assist in designing systems that do not end as the smart metering in the Netherlands.

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.

What Is a Remotely Readable and Smart Metering System?

There is not a single type of metering network. 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).

1. **Automatic Metering Readout (AMR)** allows only communication initiated by the meters and often without the possibility to send 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.
    a. Readings by an occasionally available device 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 TCP/IP Internet), 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.
    b. Readings by a permanent infrastructure: As the battery-powered meter's signal typically spans only tens or hundreds of meters and the data needs 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 the energy consumption, for example, to learn about activities that result in very high consumption.

2. **Advanced Metering Infrastructure (AMI)**, also called smart grid, e.g. by Kumar et al. (2019), 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 reliability, efficiency, and sustainability. 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).

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

1. **Metering for billing** performs the same functionality as legacy analogue metering. The goal is to meter consumption and issue a bill.
2. **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. Accident detection is another operational example. Britton et al. (2013) claim that current estimations assume customer post-meter 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 action in case of a post-meter leakage.
3. **Value-added services** let the user benefit from smart metering. For example, the user can receive suggestions on how to improve energy consumption, or the smart grid may instruct cooperative appliances in the household to use electricity at low prices during off-peak times.

Smart metering networks typically employ different protocols like ZigBee, Zwave, WiFi, MobileFi, WiMAX, powerline communication (PLC), mesh networks on unlicensed radio, 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 subject, 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 UK and the US. They identified strategies that help gain public confidence.

As discussed above, metering networks differ in complexity. Hence, each deployment may result in a different set of threats. Kumar et al. (2019) offer an overview of the threats appearing in the metering networks, 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 energies. According to Kumar et al. (2019), privacy threats are not fully understood in the metering networks. 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 can reveal household activities such as taking a shower, 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 and 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 a 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 obstacle 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. Residents later decrypt the metered values on their devices and compute costs verifiably by the energy supplier. Moreover, they 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 utility.

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 in 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) fulfils 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 advices given by Polčák & Matoušek (2022). Their advice consider a specific deployment. This chapter focuses on metering networks 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) covers the history of soft law that has clarified crucial aspects. 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 Article 29 Data Protection Working Party (GDPR transformed the working party into European Data Protection Board, EDPB). Article 29 Data Protection Working Party 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 on smart metering to the Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU). Through Programming Mandate M/487 EN, the European Commission also asked 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 are not legally binding. However, data protection regulations like GDPR are legally binding.

The Recommendation 2012/148/EU 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 GDPR recognizes that identifiers provided by devices may be used to identify them. Moreover, the Court of Justice of the European Union (CJEU) 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.

Recital 10 a11 of the Recommendation 2012/148/EU clarifies GDPR, 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.

GDPR deals with data protection impact assessment in Article 35. Recital 15 of the Recommendation 2012/148/EU argue that an assessment of the data protection impact should be carried out prior to the roll-out of smart metering systems. Recommendation 2014/724/EU later clarified the requirements for data protection impact assessment.

For completeness, let us summarize GDPR obligations. Article 4 provides definitions for basic terms like personal data, processing, controller (the entity that decides the means and purposes of the processing),

processor (an entity that processes personal data on behalf of the controller). Article 5 declares the basic rules for processing: lawfulness, fairness and transparency and puts restrictions on the processing like purpose limitation and data minimization; the controller is responsible for the demonstration of the compliance (accountability principle). Article 6 provides legal bases for processing; note that all except consent allow processing only strictly necessary personal data.

CJEU decided several cases that dealt with the condition of necessity (CJEU, C-13/16, point 30, C-92/09 and C-93/09, point 86, C-473/12, point 39, C-212/13, point 28, 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 data minimization is, see (CJEU, C-708/18, points 48-51). Case C-708/18 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 resolution 2021/C 494/11 recently evaluated GDPR. In the resolution, 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 GDPR 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.

In comparison, 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 re-identified.

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 analogue 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."* 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 more frequent 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. GDPR 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 or a smart grid need to apply. Later, the section focuses on manufacturers of smart meters.

Entity Running a Metering System

Step 1: The entity running a metering system or a smart grid (further referred to as a controller) needs to list all the operations carried out by a future metering system, a smart grid. Alternatively, a controller can carry these steps during an audit of an existing metering system or a smart grid 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 time span to detect water leakage, or analysis of patterns and energy usage to provide suggestions to reduce consumption.

Step 2: The controller must determine the data needed to achieve each selected goal. The controller should minimize the amount of 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 (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, 2016, Art. 25) and the application of technical and organizational security measures (GDPR, Article 32).

- 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 the need of frequent readouts leaving the device. There was not any Court of Justice decision directly applicable to this case but the author of this text believes that detecting events directly in the meters demonstrates compliance with the principle of data protection by design (GDPR, 2016, Art. 25). Note that data protection by design refers to the current technological state, so the controller finding that there are not any products detecting needed events on the market should be able do demonstrate the need to perform frequent readout to collect data needed to evaluate the events.

- The controller might need to decide between several possibilities how to reach the same goal. 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 meter consumption for peak and off-peak hours separately. The latter option allows the controller to read the metered consumption less frequently which demonstrates the adherance to the data minimization principle. Again, the controller can find that there is not any suitable meter offering the needed functionality; the wording of the GDPR Article 25 enables the controller to demonstrate that the market does not offer any other meter collecting sufficient data.

Step 3: The controller needs to decide the lawfulness of processing for each selected goal (GDPR, 2016, Art. 6); 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 its 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 but it can employ consumption data from a distribution network that already 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 that particular household does not exhibit fraudulent behavior.
- If there is not any other possible basis in Art. 6, 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 have their data private. As Orlando & Vandevelde (2021) and Knyrim & Trieb (2011) warn, the need of consent should be avoided for operational and billing services of the metering system. The author of this text recommends relying on a consent only exceptionally.
- If the market analysis performed in the second step revealed that the controller needs to deploy a metering device providing more frequent data than necessary needed, the controller should reevaluate if the legal basis allows such interpretation. The more disparity between the absolutely necessary frequency of reading 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 the 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).

Step 4: The controller should decide the envisaged time limits for the erasure of the collected personal data. For example, the controller is legally obliged to keep (or forward) some data from the smart meters, e.g., 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. By processing the data for a very limited time, the controller demonstrates compliance with the data minimization principle.

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

- The controller can realize that it wants 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 GDPR (2016).
- Multiple parties determine the purposes and means of the processing (GDPR, 2016, Article 26).

- 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 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU) calls for 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, C-25/17, and C-40/17. For example, Advocate General Mengozzi (2018, paragraph 68) considers that it is necessary to rely upon a factual than a formal analysis. The 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)) explicitly mentions ICT manufacturers being considered controllers of personal data.

- Polčák & Matoušek (2022) reported a case in which an association of co-owners (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) do not offer a correct answer to this question. However, had the distributor warned the association in advance that the meters perform frequent readouts and there is not legal basis for such transfers unless the inhabitants of each household give their free consent, and had the parties signed a contract in conformance with GDPR, Article 26, such contract arrangement would demonstrate the adherence to the accountability principle.

Step 6: The controller should determine technical and organizational security measures (GDPR, Article 32). The controller should focus on the availability, integrity, confidentiality, authentication, and identification of the authorized personnel, non-repudation, access control, accountability, and auditing (GDPR, Kumar et al., 2019). A typical smart metering network will be heterogeneous. The controller needs to identify the assets, responsibilities of the employees, threats, their 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 over time, and the complexity of the deployed smart grid 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.

Step 7: Once the controller successfully completes the six steps above, it determines all crucial information to create records of processing activities (GDPR, Article 30). The records of processing activities enable the controller to prepare transparent information (GDPR, Article 12-13). 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 the data access (GDPR, Article 15), rectification (GDPR, Article 16), erasure (GDPR, Article 17), restriction of processing (GDPR, Article 18), and data portability (GDPR, Article 20).

Step 8: As an additional step that is not strictly required by the data protection law but that can facilitate the deployment of smart metering, the controller should try to allow the resident to read wireless data sent by the meter.

- Such an option would demonstrate compliance with the rights for the data access (GDPR, Article 15) and data portability (GDPR, Article 20). For example, the resident may not want the controller to collect frequent readouts in case they are not necessary (Knyrim & Trieb, 2011); but the resident wants to process the readouts by 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 consumption of water when every household member is not home and all appliances like a washing machine or a dishwasher are off as a water leakage).
- Such an option improves transparency (GDPR, Article 12 and 13). The author of this paper thinks that residents that know the messages transmitted by a meter would fear less of the smart meter compared to residents left in the dark about the data collected on their household.

Manufacturers and Distributors of Components for Metering Systems

Recall that in the second and third steps, the entities running a metering system or a smart grid needed to perform a market analysis to identify meters with an adequate and preferably strict 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 smart grids, the manufacturers and distributors should clearly explain the benefits of the meters. For example, they can educate on the risk of post-meter 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). A controller determining the purposes of processing (steps 1 and 2 above) has an easier position to justify the processing if the manufacturers and distributors provide transparent and clear information.

The manufacturers should make the devices configurable. This also covers AMR deployments. Some protocols like Wireless M-Bus (EN 13757) need frequent transmissions of data. 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 the user of the meter to configure the frequency of the readouts. For example, it is technically possible to keep sending the same metered value for each transmission during a whole month.

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 envisaged time limits for erasure of the collected personal data (step 4 above, GDPR, Article 5(1)(e)). Hence, the web interface and the underlying database need to erase data after the end of 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 does 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 need to be also motivated by the data protection law. The 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)) explicitly considers ICT manufacturers as controllers pursuant to Article 4(7) [GDPR] 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 offering sufficient to the actual controllers (see also step 5 above).

CONSIDERED SCENARIOS

This section applies the data protection recommendation to three 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, e.g., 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 IT security, 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 also 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 readouts of data to comply with Directive 2018/2002/EU. For each detectable event, the controller only needs information if the event was or was not detected during the previous year.
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. The detected events will be kept for the duration of the process during which the event is explained and settled.
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 meters.

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 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 update the meters according to new requirements.

Scenario B: Permanent infrastructure of remote water readout

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 1 introduces the new processing activities. Step 4 is similar to scenario A.

Table 1. 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.

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 a freely given consent. Some tenants will participate, other will not.

Scenario C: Electrical energy grid

Knapp & Samani (2013) gives 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, by a solar panel. A household can also utilize devices that communicate with the network, for example, to negotiate the best time to consume the 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 the 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 2 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 an example of activities that can be performed.

Table 2. An example of processing activities in 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 a 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	

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 simplifies the obligations of data controllers. The key question is how to get the aggregated data. As Recommendation 2012/148/EU and European Parliament 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

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 Recommendation, Article 29 Working Party and Commission see smart metering as a foreshadowing of Internet of Things. This section reiterates through the steps suggested above in the context of IoT deployment.

Firstly, let the author of this chapter needs to clarify what IoT means in the context of this chapter. Consider a smart home consisting of appliances like smart bulbs, smart thermostats, smart plant watering, smart ovens that can notify the owner that the meal is ready, etc. Generalizing the notions of the Article 29 Working Party, its successor EDPB, European Commission, European Parliament, and CJEU cited in this paper, it is clear that these devices produce personal data. Typically, these data are propagated to the servers of the manufacturer or service provider (e.g., running in the cloud). According to GDPR, these entities are considered to be data controllers.

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, it is the customer that 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 clearly implementable. But such a rule does not exist in Europe. Consider Article 29 Data Protection Working Party 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 three 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 other deployments, some process personal data, other do not. One future research 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 functionality can help with legal certainty as well as in courts.

Kumar et al. (2019) cover well the open issues in the security area (GDPR, Article 32). According to their paper, most of the research is evaluated by simulation instead of real-world devices, but only a few evaluates their security properties with real smart meters, probably due to the limited access to real-world

devices. Another issue lies in the application of 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 lifestyle depends 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 ten percent 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 the 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 the threats and processes only necessary personal data. The chapter illustrates the application of the steps in 3 scenarios ranging from a small deployment to a full-scale grid. Moreover, the author argues that the steps can help smart home device manufacturers in designing data protection-compliant devices and services.

ACKNOWLEDGMENT (Optional)

This work was partly supported by the Brno University of Technology grant FIT-S-20-6293 (Application of AI methods to cyber security and control systems).

REFERENCES

Abreu, Z. & Pereira, L. (2022). Privacy protection in smart meters using homomorphic encryption: An overview. *WIREs*, 12(4).

Armel, K., Gupta, A., Shrimali, G., & Albert, A. (2013). Is Disaggregation the Holy Grail of Energy Efficiency? the Case of Electricity, EnergyPolicy, 52 (1).

Article 29 Data Protection Working Party (2011). Opinion 12/2011 on smart metering, available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf.

Article 29 Data Protection Working Party (2014). Opinion 05/2014 on anonymization techniques, available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Asghar, M. R., Dán, G., Miorandi, D., & Chlamtac, I. (2017). Smart Meter Data Privacy: A Survey, *IEEE Communications Surveys & Tutorials*, 19(4), 2820-2835, Fourthquarter.

Backes, M. & Melser, S. (2012). Differentially Private Smart Metering withBattery Recharging, IACR Cryptology, 183.

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

Boyle, T., Giurco, D., Mukheibir, P., Liu, A., Moy, C., White, S., & Stewart, R. (2013). Intelligent Metering for Urban Water: A Review. Water, 5(3), 1052–1081.

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.

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

California Public Utilities Commission (2014). *Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data while Protecting Privacy of Personal Data*. 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, 2014 IEEE International Conference on Pervasive Computing and Communications, 208-215.

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, 240–248, New York, NY, USA.

Court of Justice of the European Union, 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.

Court of Justice of the European Union, Case C-473/12 (2013). Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others.

Court of Justice of the European Union, Case C-212/13 (2014). František Ryneš v Úřad pro ochranu osobních údajů.

Court of Justice of the European Union, Case C-582/14 (2016). Patrick Breyer v. Bundesrepublik Deutschland.

Court of Justice of the European Union, Case C-13/16 (2017). Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA "Rīgas satiksme".

Court of Justice of the European Union, Case C-210/16 (2018). Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH.

Court of Justice of the European Union, Case C-25/17 (2018). Jehovah wittness.

Court of Justice of the European Union, Case C-40/17 (2019). Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV.

Court of Justice of the European Union, Case C-708/18 (2019). TK v. Asociaţia de Proprietari bloc M5A-ScaraA.

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

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.

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*.

Esposito, C. & Ciampi, M. (2015). On Security in Publish/Subscribe Services: A Survey, *IEEE Communications Surveys & Tutorials,* 17(2), 966-997.

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

European Parliament resolution 2021/C 494/11 (2021). 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.

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.

Kalogridis, G., Efthymiou, C., Denic, S., Lewis, T., & Cepeda, R. (2010). Privacy for Smart Meters: Towards Undetectable Appliance LoadSignatures. SmartGridComm.

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.

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

Knyrim, R. & Trieb, G. (2011). Smart metering under EU data protection law. International Data Privacy Law, 1 (2), 121–128.

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 & Tutorials,* 21(3), 2886-2927.

Lee, D. & Hess, D. J. (2021). Data privacy and residential smart meters: Comparative analysis and harmonization potential. *Utilities Policy*, 70,

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.

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

Liu, A., Giurco, D. & Mukheibir, P. (2015). Motivating metrics for household water-use feedback, *Resources, Conservation and Recycling*, 103, 29-46.

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.

McLaughlin, S., McDaniel, P., & Aiello, W. (2011). Protecting ConsumerPrivacy from Electric Load Monitoring. ACM Conference on Computer and Communications Security.

Mengozzi, P. (2018). Opinion of advocate general mengozzi. CJEU Case C-25/17, ECLI:EU:C:2018:57.

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.

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

New York State Public Service Commission (2018). *Order Adopting Whole Building Energy Data Aggregation Standard*. http://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).

Polčák, L., Matoušek, P. (2022). Metering Homes: Do Energy Efficiency and Privacy Need to be in Conflict? *Proceedings of the 19th International Conference on Security and Cryptography*, 47–58.

Programming Mandate M/487 EN (2011). Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards. European Commision. Available online at https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=472.

Recommendation 2012/148/EU (2012). *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.

Recommendation 2014/724/EU (2014). *Commision 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.

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

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.

Rial, A., Danezis, G. & Kohlweiss, M. (2018). Privacy-preserving smart metering revisited. International Journal of Information Security, 17 (1), 1–31.

Yang, W., Li, N., Qi, Y., Qardaji, W., McLaughlin, S., & McDaniel, P (2012). Minimizing Private Data Disclosures in the Smart Grid. ACM Conference on Computer and Communications Security.
Zeifman, M. & Roth, K. (2011). Nonintrusive Appliance Load Monitoring:Review and Outlook, IEEE Transactions on Consumer Electronics, 57(1).