Smart Grid Challenges through the lens of the European General Data Protection Regulation

Jabier Martinez – Alejandra Ruiz – Javier Puelles *{name.surname}@tecnalia.com*
Digital Trust Technologies (TRUSTECH) – Tecnalia
Derio, Spain

Ibon Arechalde *ibon.arechalde@tecnalia.com*
Digital Lab services – Tecnalia
Derio, Spain

Yuliya Miadzvetskaya *yuliya.miadzvetskaya@kuleuven.be*
KU Leuven Centre for IT & IP Law – imec
Leuven, Belgium

Abstract

The European General Data Protection Regulation (GDPR) was conceived to protect the privacy of individual citizens and manage the movement of personal data. The Smart Grid has the same needs as any privacy-critical system and, compared to the engineering of other architectures, has the peculiarity of being the source of the energy consumption data, which is an indirect means to infer other personal information with potential professional or commercial value. This work looks at the Smart Grid from the perspective of the GDPR, which is especially relevant now given the current growth and diversification of the Smart Grid ecosystem. We contribute a review of existing works showing the importance of energy consumption as valuable personal data, an analysis of the established Smart Grid Architecture Model regarding GDPR compliance, and a list of technical and legal challenges where we can highlight the challenge of managing the data processing by third parties.
Keywords: Smart Grid, Privacy, Data Protection, GDPR.

1. Introduction

The General Data Protection Regulation (GDPR) is in application since the 25th May 2018 to ensure the protection of individuals' rights of citizens regarding their personal data, and imposes legal obligations for the movement of such data both inside and outside of the European Union. GDPR is conceived on top of "the respect for private and family life and home"[1], and the definition of personal data includes the factors related to the "physical, physiological, genetic, mental, economic, cultural or social identity of natural persons" (Art. 4(1) of the GDPR).

Our focus is on the Smart Grid, a large ecosystem of hardware- and software-intensive systems with a large diversity of stakeholders. The Smart Grid is a world-wide challenge towards a more reliable, efficient and sustainable electrical grid. The times of manually reading or reconfiguring the electricity meter are gone and electricity distributors and suppliers are experiencing profound changes. Smart Meters automatically register and transmit the data through the Power Line Carrier (PLC) or wireless connections to data concentrators and central systems using Meter Data Management (MDM) Systems. Also, several services can be remotely applied such as changing the pricing policy or activating or deactivating the electrical service.

[1] Art. 7 and 8 of the Charter of fundamental rights of the European Union. Privacy and data protection are both recognised as fundamental rights.

All the stakeholders in the value chain can benefit from the Smart Grid: End users are empowered through near real-time information (24 hours per day, 7 days a week) that they can use to adjust their consumption or to identify a more appropriate pricing policy. Suppliers can perform profiling and provide innovative and personalized pricing policies that can be beneficial to avoid consumption peaks or waste of energy [42]. Distributors have an effective tool to better monitor and manage their networks. In addition, smart metering promises to enable "prosumers" (both producers and consumers of energy) to be more easily rewarded for their contribution. The market around the Smart Grid includes big companies but also SMEs acting as distributors or suppliers as well as a dynamic ecosystem of third-parties providing value-added services.

Data processed in a Smart Meter includes more than one thousand parameters and metrics such as the quality of the signal, but the main one is the electricity consumption which is transmitted at very small intervals of time. Prior to establishing the Smart Grid, the consumption was measured approximately each month. The privacy-related issues mainly arise now when instantaneous data can be taken. Energy consumption can be used for guessing the data subject habits, creating a personal behaviour profile, deducing personal and socioeconomic information, listing the existing electrical equipment and monitoring their usage, or guessing the presence, absence or current activity of the residents [4] [40]. Therefore, energy consumption measurements can be considered personal data providing information of an "identifiable natural person" (Art. 4 (1) of the GDPR) with great potential to be processed, solely or in combination with other data, for "professional or commercial activities" ((18) of the GDPR). Exploiting behavioral data through the Smart Grid can be motivated mainly by financial or political reasons [25].

Other personal data such as the address, contact details, bank accounts etc. can be found in the Smart Grid context. However, these mainly appear in administrative or organizational processes such as the billing process of distributors, suppliers and third parties. These cases fall in the general category of privacy challenges for information technology services. The aspect that makes the Smart Grid special regarding privacy concerns is the energy consumption, the possibility to associate it with a data subject, and the consequences of disclosing these personal data or its usage without explicit consent.

The methodology of this work consisted on several iterations to create and refine the content with Smart Grid and GDPR experts (both researchers and practitioners) from the European PDP4E project consortium (Methods and tools for GDPR compliance through Privacy and Data Protection Engineering) [33], the Digital Lab, the Digital Energy, and the Digital Trust Technologies area at Tecnalia, as well as legal experts from the KU Leuven Centre for IT & IP Law, along with a literature review using the snowballing approach [41].

This paper is structured as follows: Section 2 presents background information. Then, Section 3 presents our analysis of the Smart Grid Architecture Model regarding GDPR. Section 4 presents the challenges. Finally, Section 5 concludes this work and outlines future work.

2. Background on the Smart Grid

In this section, we provide background information on electricity consumption data, and the state-of-the-practice regarding widely accepted conceptual frameworks and the normative spaces governing the Smart Grid context.

2.1. Frequent data of electricity consumption

Electricity consumption is usually represented as a time series where time is presented in the horizontal axis and the energy consumption (in watts) is presented in the vertical axis. The shape of the time series will be then defined based on the appliances used, or not used, in the daily lives of the residents. Several techniques for time series analysis can be

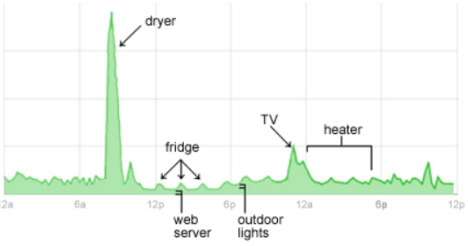

Figure 1. Illustration of a time series of electricity consumption (Source: [13])

performed such as time series classification or forecasting [24]. A taxonomy of Smart Meter data analytics is available [40]. Figure 1 is an illustrative example of a time series from the Google Power Meter project (discontinued in 2011) [13] which, once integrated with Smart Meters and with the appropriate consent, allowed users to record and visualise their own electricity consumption. We can observe how load signatures (e.g., dryer, fridge etc.) can be identified.

The simultaneous use of several appliances can make it difficult to automatically analyse time series (e.g., accumulative effect of energy consumption). However, this effect can be minimized if the load signatures were isolated at some point in time or through approximation techniques. A review by Wang et al. [40] of Smart Meter Data Analytics presents different applications of this data, and ten open data sets of Smart Meter data.

2.2. The Smart Grid Architecture Model

The Smart Grid Architecture Model (SGAM) [3] is a reference framework widely adopted by the Smart Grid community. Figure 2 is the representation of the SGAM that helps to position Smart Grid actors and use cases in a three-dimensional space of:

- Domains (Generation, Transmission, Distribution, Distributed Electrical Resources (DER) and Customer Premises),
- Zones (Process, Field, Station, Operation, Enterprise and Market), and
- Interoperability layers (Component, Communication, Information, Function and Business).

As mentioned in Section 1, Smart Meters have drastically changed this industry, notably, the SGAM Information and Communication layers have now much more importance compared to the era when the meters were not highly and continuously connected. Relatively speaking, these two layers are not yet completely mature, so crosscutting concerns such as security had inevitably gain relevance.

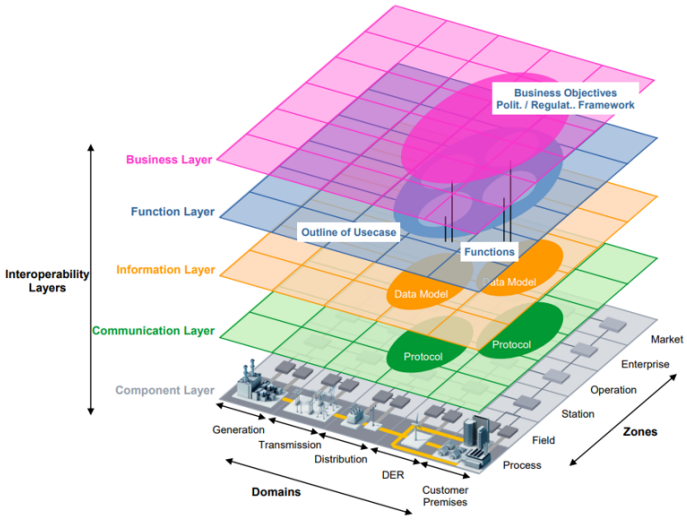

Figure 2. Smart Grid Architecture Model (Source: [3])

2.3. Normative spaces

The International Electrotechnical Commission created and maintains a standards map [18] using the SGAM as the reference conceptual framework. It currently contains information about 512 standards categorized in 16 component-related clusters. In addition, for each component, several use cases and examples are included. The standards map identifies 4 crosscutting functions: Telecommunication, Security, Electromagnetic Compatibility (EMC), and Power Quality. Another crosscutting aspect related to security is privacy which is the focus of this work.

The European Smart Grids Task Force Expert Group for Standards and Interoperability presents *My Energy Data* [12] as services which are subject to the GDPR. They also analyse the diversity of Smart Grid setups in different countries with respect to privacy. Our aim is to provide a general view without a special focus on country specificity. The Smart Grid Task Force also provides guidance for conducting Privacy Impact Assessment (PIA) through the Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems [11]. A survey on standards related to privacy in the Smart Grid identifies ten standards [23]. The two of high relevance are NISTIR 7628 [31, 32], and NIST SP 800-53 [29]. NISTIR 7628 is also mentioned in the Task Force of Privacy and Security approach at the Smart Meters Co-ordination Group as the reference for security requirements for device access control and message protection.

3. Natural persons identifiers and energy consumption through the SGAM layers

This section presents an analysis of how the identifier of the data subject and its energy consumption is propagated through the technical infrastructure and stakeholders of the Smart Grid.

3.1. Component and Communication layers

Figure 3 illustrates the Component and Communication layers of the SGAM. The Smart Meter device (bottom right) usually transfers data through the Power Line Carrier (PLC) to a Distribution Data Collector (DDC). PLC is used in some countries such as France, Spain or Italy. Others like UK or USA use wireless communications, sometimes using DDCs but others not. These DDC concentrators installed in the secondary substations, usually one per neighbourhood, are the intermediary points in the transmission to the distributor Head End System (HES) for around three hundred smart meters.

PLC does not perform well in data transmission for long distances, thus, in case of remote locations, more expensive solutions should be put in place such as Point-to-Point (P2P) protocols to send the data directly to the HES without the need of DDCs. To communicate with the HES, the DDC might use PLC, General Packet Radio Service (GPRS), other radio protocols, Digital Subscriber Lines (xDSL) or Fiber Optics. The HES communicates with the Distribution Management System (DMS) to receive the aggregated reports. Approximately, a DMS exists at national scale for each distributor. Then, already in the Enterprise SGAM zone, the DMS communicates with the Customer Relationship Management (CRM) system. The CRM system is responsible to manage and analyze the interactions with the customers. The CRM communicates with the Meter Data Management System (MDMS) of the electric distributor. This MDMS is responsible to store, manage, and analyse the vast amount of data generated in the Smart Grid. For more details we refer to a survey on Advanced Metering infrastructures [28]. A huge variety of other systems, that do not belong to the traditional distributor and supplier actors of the SGAM, appear as third parties completing the ecosystem. The MDMS can communicate with these third parties to enable or complement third-party services.

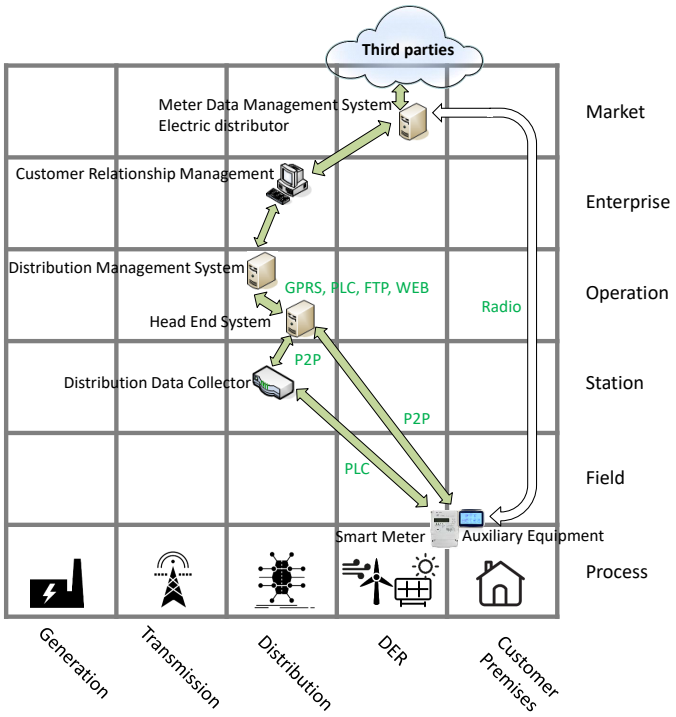

Figure 3. Component and Communication layers of the Smart Grid Architecture

Regarding the communication, the data is encrypted (e.g., AES 128 [27]) and Smart Meter devices that transmit unencrypted data are being replaced. The arrows in Figure 3 are bidirectional because central systems can remotely monitor and operate in the Smart Meter through these protocols (e.g., to respond to customer requests in real-time, to change date/hour, to modify the tariff or power demand threshold). In Figure 3, close to the Smart Meter device, the auxiliary equipment is another possible component which might directly communicate with the MDMS or with third parties. For instance, in the UK, the communication from the Smart Meter auxiliary equipment with the supplier is direct through radio, replacing the need of DDCs, HES etc. Also, electricity users can decide and consent to add auxiliary equipment to enable third-party services. This way, third parties can obtain the data without the electric distributor.

3.2. Information layer

Figure 4 illustrates the SGAM Information layer. The Smart Meter contains the customer's supply identifier. Several identifiers can be used to link a data subject with its electrical consumption, the Smart Meter serial number (unique identifier assigned to the individual piece of hardware), MAC address (Media Access Control address, a unique identifier used as a network address for the data link layer), and the CUPs (Universal Supply Point Code) which is a unique identifier for each home or business electricity supply point which does not change in case of selecting a different supplier or energy consumption tariff.

From the Field SGAM zone where the Smart Meter is located, the information moves to the Station and Operation zones where the identifiers and energy consumption data is aggregated with those of other users. Then, at the Enterprise zone, as part of the billing process, both the distributor and the supplier have the customers' physical address, the energy consumption metrics, and the smart meter identifier. Distributors and suppliers process personal data and they might transmit this information to third parties. As we can observe, the information transverses several SGAM zones, complicating the data lineage (term used to designate the management and traceability of the data life-cycle). Figure 4 shows a coarse granularity of the information flow. The presented steps could be largely expanded using more detailed Data Flow Diagrams (DFD) with privacy-related information (e.g., [5]) on specific organizational and technological settings. However, the presented information is sufficient for the understanding of the challenges.

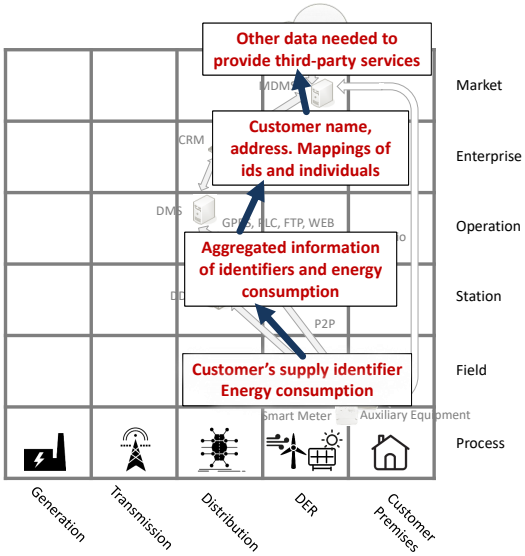

Figure 4. Information layer of the Smart Grid Architecture focused on the supply identifier and the energy consumption

3.3. Function and Business layers

Figure 5 illustrates the Function and Business layers, showing only an excerpt of all the possible functions. The data processing by the distributor or the supplier is a function related to business purposes or to improve the quality of service. The customer examining his or her consumption is also an example of function from the Customer Premises domain. Then, the data processing by third parties is a generic function referring to the diversity of current and future functions that will be available using Smart Grid information beyond distributors and suppliers.

A Spanish study on the access to the electric power consumption of Smart Meters and its access and usage by third parties [35], lists more than forty companies offering services from power consumption data. Some of them use the Smart Meter from the distributor/supplier, while others offer submetering, which means the use

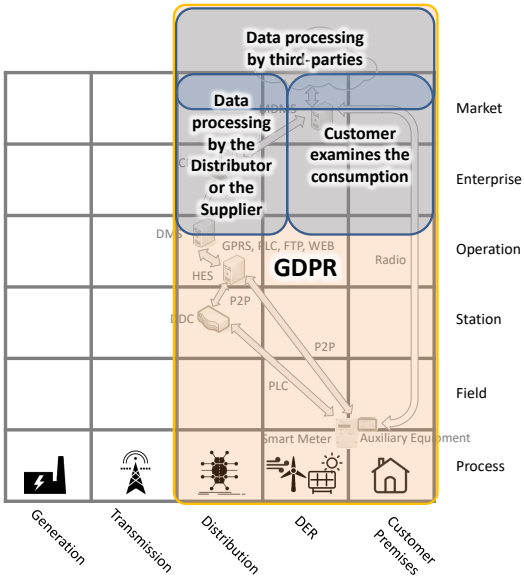

Figure 5. Functional and Business layers of the Smart Grid Architecture showing an excerpt of the possible functions and the GDPR as business normative space

of their own auxiliary equipment as mentioned in Section 3.1.

Other third parties can be related to the Internet of Things (IoT) [1]. The IoT paradigm extends physical devices and traditional real-life objects with Internet connectivity, sensors to get information about their context, and with the capacity to communicate and interact with other devices and objects to provide services. These dynamic IoT networks and the use of power consumption data are intended to unleash the promises of the Smart House or the Smart City [43]. IoT also complicates the data lineage and the use of privacy technologies, given the heterogeneity, potential mobility, and usually limited resources of IoT devices and objects [1].

As we have explained in Section 2.3, several normative spaces are placed in the different SGAM domains and zones [18], and privacy is a topic that transverses SGAM. The SGAM business layer also includes normative spaces, so we included the GDPR spanning all zones and domains, except the electricity generation and transmission domains, as they are unrelated to individuals. Other privacy-related normative spaces [23] will be similarly positioned.

4. Challenges

We categorized the identified Smart Grid challenges using the GDPR concepts that they belong to. Section 4.1 refers to the principles relating to processing of personal data, Section 4.2 elaborates on the rights of the data subject and finally, Section 4.3 presents the challenges linked with the obligations of controllers and processors. The controller is the GDPR entity determining the processing purposes and means, and who delegates the processing to the processor.

4.1. Principles relating to processing of personal data

Lawfulness, fairness and transparency

The GDPR requires controllers to process personal data in a lawful manner. It entails the need for either a legal basis, such as the existence of a contract, a legal obligation or legitimate interests, or the data subject's consent. Art. 6 of the GDPR provides the full list of possible legal grounds. In the Smart Grid scenario two potential legal grounds for the data processing are identified as the most relevant: consent and contract. The performance of a contract could, for instance, be used for the data processing necessary for the billing aspect. However, the use for marketing purposes of the data of smart grid users will quite arguable require the consent of the data subject. In all those cases the data should be collected and processed for a specific purpose and, prior to processing, the controller should opt for the most suitable lawful ground. If there are any additional purposes of processing, a controller should obtain a separate specific and informed consent from a data subject for each of them, where processing is consent based.

Smart Meter users can currently volunteer and give their consent to be monitored to receive marketing offers from suppliers or be informed about the pricing policy. Even though the transmission of the personal data to third parties can contribute to the provision of extended services or to more targeted marketing offers, the data subject shall be informed of all the recipients of his or her personal data and, where required, explicitly give their consent. Such consent can be considered freely given only if it can be as easily withdrawn as it was granted. While the Smart Grid was conceived as a new field for the launch of innovative value-added services and improvement of the sustainability of our environment, the management of the consent and handling of its withdrawal, where data is transmitted across the SGAM actors and to third parties, might encounter certain technical difficulties.

Data minimisation and purpose limitation

Since data minimisation and purpose limitation constitute the core GDPR principles, the personal data provided should be limited to what is strictly necessary in relation to the purposes for which they are processed, for instance for the performance of the contract, and for the supply and billing purposes. Thus, the controller must guarantee that third-party processors have the minimal amount of data to perform their intended processing. In contrast to other scenarios where this usually consists in not transmitting some columns from a database, the data minimisa-

tion of the energy consumption is different and requires manipulating the time series in different ways. A usual technique is to modify the resolution of the data. For example, the data with a time interval of seconds might not be needed, but maybe only each hour or just the global for a whole day or week. Some works suggest that a half-an-hour frequency is sufficiently reliable for most purposes [14], while hiding the operation states of most of the appliances. Several works also explore the trade-offs between privacy and the needs of Smart Grid data mainly by investigating different data resolution schemes and load shaping [6, 21, 37, 38, 2], but this research field is still considered to have many open challenges. In fact, the Smart Grid data minimisation is a well-studied case study for the more general problem of time series compression [7].

Data minimisation could be also performed in early phases (e.g., in the Smart Meter) considering the needs of processing in the whole chain for which the data subject gave his or her consent. Failing to guarantee data minimisation, on top of being non-compliant with the GDPR and thus exposing the controllers to fines, could have the consequence that users start adopting techniques to preserve their privacy. Known techniques are charging and discharging batteries [36] or the use of load shaping with storage and distributed renewable energy sources [21].

Special categories of data

While weather conditions stay a typical influential factor in predicting energy consumption, data fusion can contribute to more effective Smart Grid data analysis. For example, personal energy consumption prediction and forecasting can be enhanced if other data sources are combined with energy consumption histograms. The cumulative analysis of other data sources, containing various information about a data subject (location, age, gender, socio-economic parameters like the income level, employment status, educational level, whether they are property owners, the number and type of appliances) can help to establish a correlation between electricity consumption and habits. On the basis of precise energy consumption details some further assumptions can be made with regard to more sensitive aspects of personal life, such as religious beliefs and practices. According to Art. 9 of the GDPR the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs etc. is prohibited (with specific exceptions). Whereas the intense analysis of multiple data sources can improve the quality of services, it is crucial to strike the right balance between legitimate interests of controllers and the fundamental right to protection of personal data. Several studies are trying to identify which are the relevant variables that are worthy to use for the different analyses [16, 20, 26]. While some of these data sources might be discarded, others might be highly valuable for providing better or new services.

As mentioned before, energy consumption is a relevant information to satisfy the promises of the IoT. This way, the devices can decide when to charge, operate, or shut down, to be more cost and energy efficient. The automatic and unsupervised use of this data by the inter-connected devices can be problematic. The Smart Meter can be an inter-connected actor providing energy consumption measurements as well as other data such as the current pricing policy to other actors. Though coordination mechanisms between machines can be established, devices might disclose data or transfer data without consent (e.g., to the manufacturers). IoT manufacturers are very diverse and it is not possible to control which devices will be part of this configurable or self-configurable network at the design stage. Still they might need to transfer data between them (e.g., to accomplish their mission or to provide better and more efficient services), with the consequence of complicating the consent management for the data subjects each time a new device is added. The interconnected devices should be able to negotiate, preferably without human intervention, to make these networks efficient and self-managed. In addition, while the Smart Meter might be related to the controller for the energy consumption and the energy pricing policies, other IoT devices might be related to the controllers of other type of personal data, which will need to be aggregated to provide new or enhanced services.

4.2. Rights of the data subject

Right to information about processing operations

The right to information about processing operations is crucial for the exercise of all other data subject's rights. If customers of the Smart Grid are not informed about processing operations over their data at the time of its collection, they will never be aware of the use of their personal data. The lack of information will prevent them from eventually taking further decisions and actions (e.g., ask for its erasure). The GDPR stipulates that the controller shall take all the appropriate measures to inform the data subject about processing related to his or her personal data. This information shall include all the contact information about the controller, the purposes of processing operations, their legal basis and also recipients of this personal data, if any. The data subject shall be also informed if there are any intentions to transfer personal data to third parties. This information shall be provided free of charge and without undue delay. Since not all SGAM actors are known in advance, especially because of the dynamic ecosystem of third parties, it might be difficult to manage the information obligation under the GDPR.

Right to access by the data subject and right to erasure

After a data subject's request, it is technically challenging to guarantee the access (Art. 15 of the GDPR) and removal (Art. 17) of the energy consumption information from all the Smart Grid actors. As in many other scenarios, the processing chain is complex, and coordinating the processing actors and validating a complete access or removal might require advanced operations. While there is a legal permission to keep consumption data as it might be needed during the billing process, there might be difficulties with managing and separating different data sets. Therefore, the removal will have to take into account when, how and which data should be removed from each processing party. In the context of third parties related to the IoT, there might be connectivity issues that disconnects the controller from a device for long periods of time, making difficult the actual and timely access and removal of the personal data.

Right to data portability

Art. 20 of the GDPR provides for the right to data portability. When a data subject wants to change his or her electricity provider, the data portability must allow personal data to be transferred directly to the new chosen company in a practical and simple way for the end user. This might include the historic of energy consumption. Also, prior to the selection of a new company as a supplier (initiated by the user), the new potential supplier might require to perform an analysis of the personal data to identify the best personalised offer. This portability is a transfer of the individual's personal data for a specific objective where the data should be stored for a short period of time before removal. There is the risk that companies try to hide the access to personal data from other companies. To overcome this issue, a typification of consumption profiles (e.g., standardizing a predefined list of profiles) would allow data minimisation.

The right not to be subject to a decision based solely on automated processing

As set out in Art. 22(1) of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her. The wording of this provision is not straightforward and may create problems of interpretation. For instance, with regard to its scope of application. The application of this provision to the Smart Grid scenario requires a detailed analysis of all the use of personal data for profiling considerations. Moreover, there is a need to check whether a data subject might be legally affected by any decisions taken without human intervention and based solely on automated processing.

Profiling is probably the most direct use of the personal data regarding energy data consumption, and highly-personalized marketing is its most obvious commercial use. One of the main objectives of customized advertisement is to create personal profiles and cluster the profiles to maximize the probability of a successful commercial action. Apart from that, profiling and monitoring could leave the door open to other kind of uses such as guessing user personal information, or monitoring people for celebrity journalism. All these examples interfere with

the right to privacy and the right to self-determination. In the Smart Grid scenario profiling can meet the requirement of lawfulness if it is necessary for the performance of a contract between the data subject and an electricity provider, or if it is based on the data subject's explicit consent as provided in Art. 22(2) of the GDPR.

Manufacturers are interested in knowing how people use their appliances. Each appliance has an electricity load signature which can be used to differentiate its shape from other appliances. For example, in Figure 1 we observed a peak corresponding to a dryer, and smaller and periodic peaks corresponding to a fridge. If the appliance can be configured by the user or if the circumstances change, this signature can be modified to some extent. Thus, it is possible not only to know the existing appliances, but also how the residents use them. Newborough and Augood [30] illustrated this fact by showing the difference in the load signatures of the same washing machine using a 40°C cycle and a 85°C cycle. This practice of using energy consumption and appliance load signatures for nonintrusive load monitoring (NILM), or nonintrusive appliance load monitoring (NIALM) was already identified as problematic regarding privacy when the technologies enabling it started to appear [17]. As another example of how personal preferences can be obtained, automatic analysis of time series was used by Greveler et al. [15] to show how the information about which TV channel is being watched can be disclosed through Smart Meter power usage profiles. Given the brightness of the TV screen, a consumption prediction model can be defined and used for each channel, and compared with the actual consumption. This research concluded that a sample taken each 0.5 seconds during five minutes is in many cases sufficient to identify the viewed content. Thus, the interests of a person can be inferred through the viewed contents and used for professional or commercial purposes.

4.3. Obligations of controllers and processors

Data protection by design and by default and security of processing

According to Art. 24 and 32 of the GDPR, the controller and processor should implement all the necessary technical and organisation measures in order to ensure the protection of personal data and appropriate level of security. Moreover, in its Art. 25, the GDPR emphasises the principle of data protection by design and transforms it in a cornerstone obligation of the development process. However, it is difficult to translate the legal rules in the GDPR into effective software and technical mechanisms. Despite of this, the security of energy networks is closely intertwined with risks to the fundamental rights to data protection and privacy. The Smart Meters constitute a part of a massive "attack surface" and are exposed to security failures. The TACIT project [39] studied the different cyber-attacks that can take place in a Smart Grid scenario. As electricity supply impacts other critical infrastructures, the cybersecurity threat to the energy sector has an effect on the whole society. Addressing data protection considerations from the design of the meters, and from all the SGAM levels, can contribute to a stronger cybersecurity.

Cyber-attacks have caused important problems for the energy sector, and the European Union has tried to address the issue with the Network and Information Security (NIS) Directive [10] that increases the harmonization of national laws of Member states. However, since the directive requires the transposition into national laws, some discrepancies will still remain. While the directive also applies to the energy sector and contains in its annex a list of energy sector organisations that could be considered as operators of essential services, it does not specify the appropriate measures and risk mitigation strategies that should be taken in order to reinforce security. According to Art. 4(1) of the NIS Directive, a risk is "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems". Therefore, energy providers should implement a threat and risk management system, establish an effective incident response network, improve resilience to cyber-attacks and ensure technical and human intervention in order to address such issues [8]. Moreover, the European Commission has provided the Smart Grid industry with recommendations on how to address such risk impact assessments [11].

Convergent security analysis (physical and digital) is needed to guarantee the security of processing of personal data as referred to in Art. 32 of the GDPR. NIST [31] refers to it as combined cyber-physical attacks, and they can affect also privacy concerns. Smart Meters are usually located in a shared place for several apartments. As examples of security threats on a Smart Grid scenario, we can mention physically accessing the Smart Meter, watching the visible display with the counter, observing the residence or identifying the names in the post boxes. These are actions that can reveal the mapping between energy consumption and the associated person. Less populated areas present more technical problems regarding these threats. Smart Meters do not need visible displays, but they are equipped with them. They usually include a LED which blinks more when the power consumption is higher. This could be used, not only to guess the power consumption, but also to associate a Smart Meter with a person if we can link the physical observation of the residence with the visible displays or the blinking of the LED for singling out an apartment. While this kind of activity seems to be more related to sophisticated preparation of criminal activities, their usage for professional or commercial purposes might not be discarded. Also, the operators from the distributor or the supplier have access to various personal information, so privacy adherence by operating personnel must be guaranteed.

Even if the Smart Meters themselves are fully compliant with the law, their connection to other devices makes them more vulnerable. Vulnerability is exacerbated by the low security standards implemented on some IoT devices [1], so manufacturers should provide for stronger safeguards from the design stage. Recall that controllers are obliged to choose manufacturers that provide for privacy-friendly solutions. Personal data within IoT devices can be available to persons that are not authorized for it, and without the consent of the data subject. Also, Cyber-Physical Systems (CPS) [34] are highly present in the Smart Grid, and it is considered that security and privacy are hindering the development of CPS in the Smart Grid context since user actions can be monitored or devised from the data that CPS manage [19].

Data breach management

Apart from data breaches that can happen in any information system, there is a special aspect of the Smart Grid. This is related to the fact that energy availability might have more priority than data subject privacy. Under the condition that such measures are proportionate and transparent, public safety will often overrule protection of personal data. For example, Denial-of-Service (DoS) attacks (e.g., sending large amounts of data so that the device is overloaded and it is incapable of answering legitimate requests) have more priority than Man in the middle/Sniffing and intrusion to the servers [39]. DoS has higher priority because the availability of electricity is safety-critical. Safety-critical systems are those whose failure can cause injury or death to people or harm to the environment in which they operate [22]. In other scenarios such as a non-critical web page providing some service, a data breach can be stopped by shutting down the service until the security patch is in place. In the Smart Grid, shutting down the availability of electricity can have uncontrolled or catastrophic consequences (e.g., hospitals or other critical infrastructures connected to the Smart Grid might be affected). The trade-offs between disclosing personal data or cutting off the electricity should be investigated with appropriate risk assessments (e.g., the Data Protection Impact Assessment mentioned in the GDPR). In a hypothetical case of a data breach, a higher priority may be given to the availability of the service. Microgrid operations or islanding (autonomously providing power to a location without being connected to the main electrical grid) is being investigated to mitigate cyber-attacks and cascading effects [9, 31]. Additionally, operators are asked to report incidents that affect the security, integrity and confidentiality of the service, if such incidents have a significant disruptive effect on the provision of an essential service. Regarding personal data disclosure, the impact on data subjects will need to be assessed, and data subjects or authorities will need to be informed depending on the risk assessment and the severity of the risk.

5. Conclusions

We analyzed the relation between the General Data Protection Regulation (GDPR) and the Smart Grid to present a characterization of the Smart Grid layers with respect to the GDPR, as well as a description of the Smart Grid challenges with respect to GDPR concepts and principles. The distributor and supplier are not the only affected actors, but also the growing and diverse ecosystem of third parties providing extra services. The challenges include the large amounts of information that can be obtained from the Smart Meter giving precise profiles of individual citizens, the assurance and minimization of the data flows, as well as the consent management before transmitting personal data to third parties. In the Smart Grid scenario, profiling is extended to larger proportions since one can single out what the person is doing every hour of the day. This is an important interference to the right to data protection, the right to privacy and the right to self-determination. As further work, Smart Grid challenges will be addressed at technical level, by providing tools and methods that can help to evidence GDPR compliance.

Acknowledgments

This work is funded by the PDP4E project, H2020 European Project Number: 787034. We would like to thank all PDP4E project partners for their valuable inputs and comments, and other individuals such as Marta Castro and Mikel Vergara for their discussions.

References

1. Bandyopadhyay, D., Sen, J.: Internet of Things: Applications and Challenges in Technology and Standardization. Wirel. Pers. Commun. 58 (1), 49–69 (2011)
2. Cárdenas, A.A., Amin, S., Schwartz, G., Dong, R., Sastry, S.: A game theory model for electricity theft detection and privacy-aware control in AMI systems. In: Allerton Conference on Communication, Control, and Computing. pp. 1830–1837. IEEE (2012)
3. CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture. (2012)
4. Chicco, G.: Customer behaviour and data analytics. In: 2016 International Conference and Exposition on Electrical and Power Engineering (EPE). pp. 771–779. (2016)
5. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering. 16 (1), 3–32 (2011)
6. Eibl, G., Engel, D.: Influence of Data Granularity on Smart Meter Privacy. IEEE Trans. Smart Grid. 6 (2), 930–939 (2015)
7. Eichinger, F., Efros, P., Karnouskos, S., Böhm, K.: A time-series compression technique and its application to the smart grid. VLDB J. 24 (2), 193–218 (2015)
8. Energy Expert Cyber Security Platform: Cyber Security in the Energy Sector, Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector. (2017)
9. EU H2020: EU funding for energy beyond the "Secure, Clean and Efficient Energy" challenge. (2017)
10. European Parliament and Council: NIS Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016. (2016)
11. European Smart Grids Task Force: Data protection Impact assessment template for smart grid and smart metering environment. (2014)
12. European Smart Grids Task Force: My Energy Data. (2016)
13. Google: Google PowerMeter. (2011) `https://en.wikipedia.org/wiki/Google_PowerMeter` Accessed June 28, 2019
14. Granell, R., Axon, C.J., Wallom, D.C.H.: Impacts of Raw Data Temporal Resolution Using Selected Clustering Methods on Residential Electricity Load Profiles. IEEE Transactions on Power Systems. 30 (6), 3217–3224 (2015)
15. Greveler, U., Justus, B., Loehr, D.: Multimedia content identification through smart meter power usage profiles. In: in Computers, Privacy and Data Protection (CPDP). (2012)
16. Han, Y., Sha, X., Grover-Silva, E., Michiardi, P.: On the impact of socio-economic factors on

power load forecasting. In: 2014 IEEE Int. Conference on Big Data. pp. 742–747. (2014)
17. Hart, G.W.: Residential energy monitoring and computerized surveillance via utility power flows. IEEE Technology and Society Magazine. 8 (2), 12–16 (1989)
18. International Electrotechnical Commission: Smart Grid Standards map.
19. Karnouskos, S.: Cyber-Physical Systems in the SmartGrid. In: 2011 9th IEEE International Conference on Industrial Informatics. pp. 20–23. (2011)
20. Kavousian, A., Rajagopal, R., Fischer, M.: Determinants of residential electricity consumption: Using smart meter data to examine the effect of climate, building characteristics, appliance stock, and occupants' behavior. Energy. 55 184–194 (2013)
21. Kement, C.E., Gultekin, H., Tavli, B., Girici, T., Uludag, S.: Comparative Analysis of Load-Shaping-Based Privacy Preservation Strategies in a Smart Grid. IEEE Trans. Industrial Informatics. 13 (6), 3226–3235 (2017)
22. Laprie, J.C.C., Avizienis, A., Kopetz, H. eds: Dependability: Basic Concepts and Terminology. Springer-Verlag, Berlin, Heidelberg (1992)
23. Leszczyna, R.: Cybersecurity and privacy in standards for smart grids - A comprehensive survey. Computer Standards & Interfaces. 56 62–73 (2018)
24. Liao, T.W.: Clustering of time series data - a survey. Pattern Recognition. 38 (11), 1857–1874 (2005)
25. McDaniel, P., McLaughlin, S.: Security and Privacy Challenges in the Smart Grid. IEEE Security and Privacy. 7 (3), 75–77 (2009)
26. McLoughlin, F., Duffy, A., Conlon, M.: Characterising domestic electricity consumption patterns by dwelling and occupant socio-economic variables: An Irish case study. Energy and Buildings. 48 240–248 (2012)
27. Miller, F.P., Vandome, A.F., McBrewster, J.: Advanced Encryption Standard. (2009)
28. Mohassel, R.R., Fung, A., Mohammadi, F., Raahemifar, K.: A survey on Advanced Metering Infrastructure. International Journal of Electrical Power & Energy Systems. 63 473–484 (2014)
29. National Institute of Standards and Technology (NIST): NIST SP 80053 Rev.4 Recommended Security Controls for Federal Information Systems and Organizations. (2013)
30. Newborough, M., Augood, P.: Demand-side management opportunities for the UK domestic sector. IEE Proceedings - Generation, Transmission and Distribution. 146 (3), 283–293 (1999)
31. NIST: NISTIR 7628: Guidelines for Smart Grid Cyber Security: Volume 2, Privacy and the Smart Grid.
32. NIST: NISTIR 7628: Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements.
33. PDP4E Project: Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering. (2018) https://www.pdp4e-project.eu. Accessed June 28, 2019
34. Rajkumar, R., Lee, I., Sha, L., Stankovic, J.A.: Cyber-physical systems: the next computing revolution. In: DAC. pp. 731–736. ACM (2010)
35. Salas, P.: Acceso a los datos de consumo eléctrico de los contadores digitales y su uso. Estudio del caso en España y propuestas de mejora para hacer posible el acceso a los datos a terceras partes. (2017) https://tinyurl.com/y4gwvrud. Accessed June 28, 2019
36. Salehkalaibar, S., Aminifar, F., Shahidehpour, M.: Hypothesis Testing for Privacy of Smart Meters with Side Information. IEEE Transactions on Smart Grid. 1–1 (2018)
37. Sankar, L., Rajagopalan, S.R., Mohajer, S., Poor, H.V.: Smart Meter Privacy: A Theoretical Framework. IEEE Trans. Smart Grid. 4 (2), 837–846 (2013)
38. Savi, M., Rottondi, C., Verticale, G.: Evaluation of the Precision-Privacy Tradeoff of Data Perturbation for Smart Metering. IEEE Trans. Smart Grid. 6 (5), 2409–2416 (2015)
39. TACIT Project: Threat Assessment framework for Critical Infrastructures proTection. (2016) https://www.tacit-project.eu. Accessed June 28, 2019
40. Wang, Y., Chen, Q., Hong, T., Kang, C.: Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges. CoRR. abs/1802.04117 (2018)
41. Wohlin, C.: Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: EASE '14. pp. 38:1–38:10. ACM (2014)
42. Yang, J., Zhao, J.H., Luo, F., Wen, F., Dong, Z.Y.: Decision-Making for Electricity Retailers: A Brief Survey. IEEE Trans. Smart Grid. 9 (5), 4140–4153 (2018)
43. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for Smart Cities. IEEE Internet of Things Journal. 1 (1), 22–32 (2014)