ComForEn 2021

Data management in energy communities

Stephan Cejka, Siemens AG Austria, stephan.cejka@siemens.com

Abstract – Following the introduction of energy communities in European law, they are now transposed into the national laws of the member states. Previous research in this area has focused on various aspects, but not yet on data processing and data protection in the community itself. For the timely allocation of the generated energy to consumers within the community, necessarily energy data needs to be accessed in a high frequency that is shown to be problematic in terms of privacy. Operation systems for energy communities thus need to adhere to the principles of the GDPR. Main responsibilities regarding data acquisition and transfer are among the duties of the distribution system operator. However, for future use cases, the current legal status may not be sufficient.

1. Introduction

Energy communities have been introduced by two directives of European Union's ‘Clean Energy Package for All Europeans’ which need to be transposed by the member states into their national laws. Thus, member states are – on the one hand – in different states of the transpositions processes, where some countries have not yet started with their legislative processes. On the other hand, the implementations in the various member states differ in their details [1] [2] [3]. In Austria, energy communities have recently been introduced by the 'renewables expansion act (*Erneuerbaren-Ausbau-Gesetz*)' in July 2021 [4]. While the Austrian law mainly focuses on the duties of the distribution system operator (DSO), and partly the connection of the DSO with the energy community, collaboration within them is not regulated.

Energy communities aim to jointly produce, consume, store, and share energy to increase the self-consumption of locally generated energy, but they could also offer other energy-related services. They have already been recognized by several national energy and climate plans as important players towards the energy transition [5]. Thus, they may become an essential element of the energy system to contribute to abating the effects of climate change as well as to provide local countermeasures against blackouts. Figure 1 shows the abstract structure of an energy community; the dashed lines show the energy flow, the solid lines show the cash flow. Relevant data are generated at all depicted levels; they are processed and stored inside and outside the energy community.

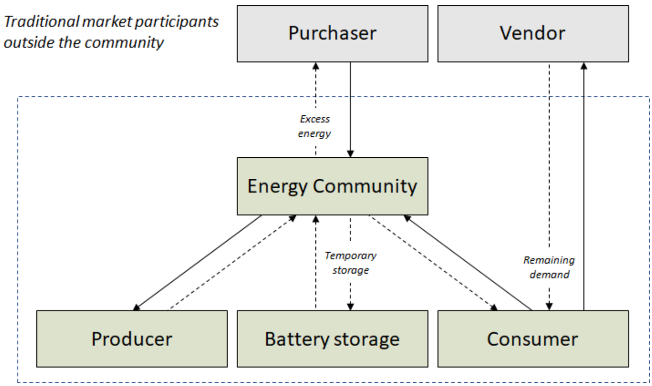

Figure 1: Structure of an energy community [3]

Recent research dealt with various aspects on energy communities (e.g., [1] [2] [3] [4] [6] [7]); for example, the differences between national implementations in the member states, which of the energy communities' variants to choose, restrictions on participation, profitability aspects, legal forms, necessary contractual relations, as well as business models and technical solutions. In this regard, the ongoing international *CLUE* project[1] as well as the national *ECOSINT* project[2] evaluate energy communities from interdisciplinary points of view (technical, legal, economical etc.). No significant focus has yet been laid on data flow and data protection aspects; initial considerations shall be the focus of this article.

[1] https://project-clue.eu/
[2] https://ecosint.at/

2. Energy data are personal data

For a timely allocation of the produced energy and the subsequent billing, it is necessary to determine energy generation and consumption data in near real-time. However, details on the individual energy consumption – especially in a high reading frequency – can provide deep insights into presence and absence, device usage, a household’s economic situation, preferences, and lifestyle [8]. Initially, neither European nor Austrian energy laws laid a focus on data protection, while it is now – at least – explicitly mentioned to be an important aspect to consider. The General Data Protection Regulation (GDPR) defines ‘personal data’ as any information relating to an identified or identifiable natural person (‘data subject’). Therefore, energy consumption data are categorized as personal data and the GDPR is thus applicable. There are several articles on data protection issues in intelligent power networks (smart grids), especially when using intelligent power meters (smart meters); various solution approaches were summarized in [8]. Thus, equipping households with smart meters have always been seen sceptically from data protection sides.

European Union's Energy Directive demands a rollout to at least 80 % of the metering points due 2024, while Austria legally specified to eventually reach 95 %. However, so far, the rollout in some regions of Austria has still been slow, at the end of 2020, less than 30 % have been reached [3]. DSOs are now legally required to equip energy communities' participants with smart meters within two months. Generally, despite equipped with a smart meter, the energy consumption of a ‘normal’ household will be metered only once a day. There is even a legally stipulated opt-out option from smart metering, which is, however, not applicable to members of energy communities. Furthermore, generally, for a quarter-hourly read-out of energy consumption data there must be an explicit opt-in (i.e., either by using a special tariff requiring such data, or by special desire). However, for energy communities’ participants this read-out interval is legally explicitly defined and cannot be avoided. For the scope of this article, the relevant nationally defined legal minimum requirements for smart meters are in particular:

- meter readings, average power values, and energy consumption values are measured and saved in an interval of 15 minutes,
- all data recorded by midnight are transmitted to the DSO once a day by noon of the following day at the latest,
- smart meters are equipped to be able to communicate with external devices in the customer’s sphere via a communication interface,
- devices and their communication are secured and encrypted according to the state of the art, and
- devices must comply with data protection regulations according to the state of the art.

As an additional aspect in terms of data protection law, the collected data will not only be made available to the DSO and the suppliers, but also to the energy community. The expected small number of participants, as well as the limited geographical operational area needs to be considered as this configuration simplifies to ‘know the face related to the personal data’.

3. Technical implementations

The implementation of energy communities requires suitable (IT) systems, including for allocation of available energy to the consumers as well as the correct billing. In anticipation of the national implementation of the directives, recent research dealt with a prototypical technical implementation using blockchain technology [6]. Indeed, the directives provide a definition for 'peer-to-peer transactions' that leads into the direction of blockchain technology [9]. Its use simplifies the peer-to-peer energy trading among its participants by utilizing smart contracts [9], but it particularly raises privacy concerns and challenges due to their technology-immanent design principles (data once saved on the blockchain is inherently immutable and eternal) [10] [6]. It is neither easy to answer who is the person responsible for data protection in a blockchain system, nor how GDPR's data subjects' rights (information, access, rectification, and erasure rights) can be ensured [10]. Despite those considerable issues, a data protection-friendly prototypical implementation (e.g., use of pseudonyms, user rights management, initiate a new blockchain after each billing cycle etc.) was described in [6].
However, real implementations do not necessarily have to be based on blockchain technology; the *CLUE* and *ECOSINT* projects will also investigate technical implementations of energy communities aside the blockchain. For example, *CLUE* suggests a toolkit consisting of [11]:

- a **planning tool**: to plan the community to integrate renewable energy sources, customers, electric mobility, storage, and power-to-heat applications,
- a **monitoring and information tool**: to provide capabilities for a real-time overview of the community, e.g., the energy flow within the community,
- an **operation tool**: the event-based operation environment with fully automated services for analyses and alarming.

4. Responsibilities of the DSO

The DSO is responsible to

1. **measure** the generated and consumed energy in a quarter-hour interval,
2. **allocate** the generated energy to the participants according to the agreed model, and
3. **provide the data** to the energy community.

4.1 Measure energy data

Each participant is required to be equipped with a smart meter; there is no possibility to opt-out. The quarter-hour measurements are collected at least once a day by the DSO (cf. Sect. 2).

4.2 Allocate energy

Energy generated in the energy community needs to be allocated to the consumers. Surpluses are fed into the public network and assigned to the supplier with whom a purchase agreement has been concluded. Legally there are two options available for the allocation, one of which needs to be chosen at the creation of the energy community and disclosed to the DSO:

- the **static model**: The same share of energy is assigned to each participant at each time (i.e., quarter hour). If the assignment exceeds the current consumption of a participant, the remaining energy is fed in, even if other participants would require more energy than assigned.
- the **dynamic model**: Energy is assigned to each participant according to its consumption at that time (i.e., quarter hour). Only the remaining energy that is not required at that time by any participant is fed in.

	Required energy	**Static model**	**Dynamic model**
Production		4 kWh	4 kWh
Consumer 1	1 kWh	1 kWh	1 kWh
Consumer 2	3 kWh	2 kWh	3 kWh
From supplier		1 kWh (remaining from C2)	-
To supplier		1 kWh (remaining from C1)	-

While the static model is easier to understand, the dynamic model is more economic, and it optimizes the internal consumption of the community. The allocation of energy to the members is among the duties of the DSO; thus, neither the producer nor the energy community can influence which participant gets which amount of the energy.

4.3 Provide data

The recorded quarter-hour values are transmitted to the suppliers and the energy community as soon as possible, but at latest on the next day. They shall be provided in a customer friendly way in a web-portal but/and (also?) in a machine-readable format. While there are specific rules for the data transfer and data protection between DSO and suppliers, detailed rules for energy communities are (currently) missing. Thus, there is a defined communication transfer and format between DSO and suppliers, but not (yet) between DSO and energy communities.

5. Operation of energy communities

According to the law, the community participants are required to agree on "the data management and data processing of energy data of the producing systems and the consuming systems of the participants *by the DSO*". This policy is seen critical: On the one hand, the participants of the energy community cannot decide on how and to what degree the DSO is permitted to operate on energy data. On the other hand, the energy community itself needs to find a consent on how it operates on data.

As described, energy communities shall not only be able to produce, consume, store, and share energy; they could also provide ‘other’ energy-related services. After an initial phase, energy communities are expected to increasingly pursue more advanced use cases beyond the simple allocation and billing of generated energy to its participants. In those use cases, the stipulated limited options of either a static or a dynamic allocation, as well as to receive energy production and consumption data not before the next day might not be sufficient. Furthermore, these use cases could require data in a more frequent interval than quarter-hour values. A higher interval read-out by the DSO is not permitted by law, and a more frequent transfer of the collected data to the energy community is not stipulated.

Energy communities could thus utilize the customer interface of the smart meters, where real-time data is available to the customer. For the usage of such intrinsic data by the energy community, a legal justification is required; applicable would either be:

- the data subject has given **consent** to the processing of his or her personal data for the specific purpose, or
- processing is necessary for the performance of a **contract** to which the data subject is party, such as the energy community’s operational agreement.

In cases, where the energy community pursues advanced use case that require data in a high frequency the processing is necessary. It can, however, also be argued that participants without consent may profit from the basic use cases, but not from the advanced ones, if their operation can be reasonably distinguished.

In any case, operation systems for energy communities must adhere to the principles of the GDPR; among them, and especially to mention in this context are:

- the **data minimisation** principle: data acquisition must be limited to the extent necessary for the purposes; only the minimum personal data required for the specific application must be collected,
- the **storage limitation** principle: data must be stored only for as long as necessary for the purposes, and
- the **integrity and confidentiality** principle: processing of data must adhere to appropriate security using technical and/or organizational measures.

As the GDPR contains sensitive fines, compliance with obligations of the GDPR is important.

The primary subject for the lawful processing of data and compliance with the GDPR is the ‘controller’, who is responsible for adherence to the principles, and to ensure and fulfil the data subject's rights. The controller continuously assesses the risks posed by the processing operations and takes appropriate technical and organizational measures to ensure the adequate protection of privacy. Especially the mentioned principles and the data subject rights may conflict with implementations utilizing blockchain technology (cf. Sect. 3) [10] [6]. The controller is not required to be a natural person, thus the energy community itself – required by law to be incorporated in some legal form [4] – will be the controller.

A further question in regards of the GDPR is whether a data protection officer (DPO) needs to be designated. This is suggested, if 'the core activities of the controller […] consist of processing operations which […] require regular and systematic monitoring of data subjects on a large scale'. The obligation to nominate a DPO within the community would be a burden; however, it shall be mentioned that – like third parties can be appointed for any parts of the community's operation – also the DPO does not need to be a member of the community.
To further foster compliance with data protection obligations, two remarkable concepts are included in the GDPR:

- **Privacy by design**: New inventions shall be designed in a way that privacy is considered from the beginning and not as a subsequent add-on; thus, systems conform to the GDPR at every time. The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures to meet the requirements of the GDPR and protect the rights of data subjects. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
- **Data protection impact assessment (DPIA)**: An evaluation to reduce the risks of misusing personal data shall be conducted. In particular, the execution of a DPIA is appropriate if new technological solutions are used, if data processing is carried out on large scale or if automated processing leads to decisions that have a legal effect for natural persons, all of which may be applicable to energy community operations. A DPIA provides evidence that appropriate measures have been taken to protect personal data.

6. Conclusion

Data acquisition, usage and privacy have not been in the focus of the beginning research on energy communities. Now, with available national implementations and thus the possibility to start communities, those aspects will come to the fore. The main purpose of this research article was to provide initial considerations on this topic, while it will necessarily need to be further considered throughout the next years.

Acknowledgments

Funding by the Austrian Research Promotion Agency (FFG) under project no. 881165 (ECOSINT) is gratefully acknowledged.

References

[1] M. E. Biresselioglu, S. A. Limoncuoglu, M. H. Demir, J. Reichl, K. Burgstaller, A. Sciullo and E. Ferrero, “Legal Provisions and Market Conditions for Energy Communities in Austria, Germany, Greece, Italy, Spain, and Turkey: A Comparative Assessment,” *Sustainability,* vol. 13, no. 20, p. 11212, 2021.

[2] D. Frieden, A. Tuerk, C. Neumann, S. d'Herbemont and J. Roberts, “Collective self-consumption and energy communities: Trends and challenges in the transposition of the EU framework,” 2020.

[3] S. Cejka, D. Frieden and K. Kitzmüller, “Implementation of self-consumption and energy communities in Austria’s and EU member states’ national law: A perspective on system integration and grid tariffs,” in *26th International Conference on Electricity Distribution (CIRED),* 2021.

[4] S. Cejka and K. Kitzmüller, “Rechtsfragen zur Gründung und Umsetzung von Energiegemeinschaften,” in *12. Internationale Energiewirtschaftstagung (IEWT),* 2021.

[5] J. Roberts and C. Gauthier, “Energy communities in the draft National Energy and Climate Plans: encouraging but room for improvements,” 2019.

[6] S. Cejka, F. Zeilinger, M. Stefan, P. Zehetbauer, A. Veseli, K. Burgstaller and M.-T. Holzleitner, “Implementation and Operation of Blockchain-Based Energy Communities Under the New Legal Framework,” in *Smart Cities, Green Technologies, and Intelligent Transport Systems,* C. Klein, M. Helfert, K. Berns and O. Gusikhin, Eds., Cham, Springer International Publishing, 2021, pp. 3-30.

[7] B. Fina and H. Fechner, “Transposition of European Guidelines for Energy Communities into Austrian Law: A Comparison and Discussion of Issues and Positive Aspects,” *Energies,* vol. 14, no. 13, p. 3922, 2021.

[8] S. Cejka, F. Knorr and F. Kintzler, “Privacy issues in Smart Buildings by examples in Smart Metering,” in *25th International Conference on Electricity Distribution (CIRED),* 2019.

[9] S. Cejka, K. Poplavskaya, C. Monsberger and M. Stefan, “Blockchain technology and peer-to-peer trading in energy communities: A regulatory perspective,” in *1st IAEE Online Conference*, 2021.

[10] M. Holzleitner, K. Burgstaller, S. Cejka and A. Veseli, “Electricity trading via Blockchain in an energy community from a data protection point of view,” *European Energy and Climate Journal (EECJ),* vol. 10, pp. 31-41, 9 2020.

[11] S. Cejka, A. Einfalt, K. Poplavskaya, M. Stefan and F. Zeilinger, “Planning and operating future energy communities,” *CIRED - Open Access Proceedings Journal,* vol. 2020, pp. 693-695, 2021.

Mag.iur. Dipl.-Ing. Stephan Cejka received his bachelor’s degree (BSc) in Software & Information Engineering in 2013 and his master’s degree (Dipl.-Ing.) in Software Engineering & Internet Computing in 2019, both from Vienna University of Technology. Additionally, he received his magister degree (Mag.iur.) in Laws from the University of Vienna in 2016. Stephan Cejka joined the department for Corporate Technology of Siemens AG in 2014, where he works as a research scientist in a research group for smart grids and smart buildings. His research interests include distributed systems in the smart grid and smart building context, energy communities and interdisciplinary aspects in energy laws and energy informatics (e.g., privacy issues) within these fields.