Personal Energy Administration Kiosk Application

An ICT-ecosystem for Energy Savings through Behavioural Change, Flexible Tariffs and Fun

Contract No 695945

Deliverable D5.1

Privacy issues and consumer rights

Prepared by Marie Holzleitner (EI-JKU)

Version 1.0: 10 July 2018

Table of contents

1. Introduction 4
2. New EU data protection law 6
3. Data protection and smart meters: the GDPR and the “Winter Package” 8
3.1. ICT system “device application” 10
4. Scope of application of the GDPR 13
4.1. Material scope 13
4.1.1. Definition of “energy data” 15
4.2. Territorial scope 18
4.3. Personal scope 19
4.3.1. The data subject 19
4.3.2. Controller and commissioned processor 19
4.4. Data management and assignment of responsibilities 21
5. The main processing activities of each actor in the energy sector 24
5.1. Suppliers 24
5.2. Distribution system operators 26
5.3. Transmission system operators 32
5.4. Energy generators (producer) 33
5.5. Meter operators 34
5.6. Energy service companies 34
6. Principles and lawfulness of processing 35
6.1. Principles of data processing - Art. 5 GDPR 35
6.1.1. Legality, good faith, transparency pursuant to Art. 5 (1) (a) GDPR 35
6.1.2. Purpose-based processing pursuant to Art. 5 (1) (b) GDPR 35
6.1.3. Data minimisation pursuant to Art. 5 (1) (c) GDPR 35
6.1.4. Correctness pursuant to Art. 5 (1) (d) GDPR 36
6.1.5. Storage limitation pursuant to Art. 5 (1) (e) GDPR 36
6.1.6. Integrity and confidentiality pursuant to Art. 5 (1) (f) GDPR 36
6.2. Lawfulness of data processing - Art. 6 GDPR 36
6.2.1. Consent 37
6.2.2. Legitimate interest in processing 38
6.2.3. Further processing 39
6.3. Rights of data subjects 40

6.3.1. Art. 12 to 16 GDPR – The right to information 40
6.3.2. Art. 17 GDPR – Right to deletion, right to be forgotten 45
6.3.3. Art. 18 GDPR – Right to restriction of processing 46
6.3.4. Art. 21 GDPR – Right to objection 47
6.3.5. Art. 22 GDPR – Profiling and automated decision-making 47
7. Data protection impact assessment and prior consultation 49
7.1. Art. 35 GDPR Data protection impact assessment 49
7.1.1. Definition 50
7.1.2. When is a DPIA required? 51
7.1.3. DPIA process 53
8. Art. 20 GDPR – Right to data portability 55
9. Conclusions 59
10. Bibliography 61

Description of work

This task addresses legal issues around the exploitation of 15-minute load profiles of households through the ICT-to-Human ecosystem. It is important that the usage of the data is transparent and that users understand what happens with their data, i.e. who has access to it and for what reason. Furthermore, the user needs to be able to restrict exploitation of her or his data and needs full power to request deletion of the entire data set. EI-JKU is among the most experienced institutions with respect to national and EU-wide data protection (see Section 1.3.4 and Chapter 4). Legal experts will ensure that all data protection and consumer rights issues will be handled in the most careful manner during the runtime of the field tests, and will give recommendations on how these critical issues should be addressed in a real market roll-out. The methods of choice in the context of legal research are the analysis of legal documents and consultation with selected representatives of data protection agencies. Furthermore, the legal experts in the consortium have to report their results to the Privacy Protection Advisory Board (PPAB) regularly.

The ICT-to-Human ecosystem is hosted by the electricity provider. One of the great advantages over systems being hosted by the grid operator is the portability of the system when households moves into a new residence. To facilitate a smooth and uncomplicated transfer of user-related historical data, benchmarks, and achievements in serious gaming, etc., to the new location, this has to happen under an unambiguous legal framework to ensure privacy and a secure transfer of the data. The legal team of PEAKapp will draw a clause for the standard business conditions of the service contract with the provider that ensures the above formulated consumer rights. The work on regulation done in this work package (see Task 5.3) will then analyse the need for making this clause a legal requirement for electricity providers, similar to rights of distribution system operators to grant consumers access to their load profiles.

1. Introduction

The following work package[1] deals with the use of energy consumption data in the context of ICT systems. It is important that the use of data is transparent and that users understand what happens to their data, i.e. who has access to it and for what reason. In addition, users must be able to restrict the use of their data and be able to request the deletion of the entirety of their data set. Through the new General Data Protection Regulation (GDPR)[2] the exercise of these rights is greatly facilitated.

The GDPR provides a high level of protection for the personal data of EU citizens. The GDPR applies directly from 25/05/2018 in all EU countries directly and affects companies worldwide who are active in the European market.

As personal data can be used to draw conclusions about identified or identifiable persons, this new regulation aims to ensure the control of EU citizens over their personal data in the digital world.

The GDPR requires a high degree of data security. In order to ensure an appropriate level of data protection, appropriate technical and operational measures must be taken, in particular regarding appropriate IT solutions, privacy statements, audits and employee training. In addition, data processing activities must be documented. The requirements for data processing consent have become more stringent so that the tacit granting of consent by silence or by “prior clicking” of the corresponding consent is no longer possible. Certain data protection violations are to be reported to the supervisory authority. In addition, certain organisations, such as government agencies, banks, insurance companies, telecommunications service providers, hospitals and health centres, are required to appoint a data protection officer.

In addition, every entity addressed by this regulation must be informed about it and prepared. Data protection law applies to every organisation because they all necessarily deal with personal data. Typical data processing activities include the collection and use of employee and customer information, application materials, the sending of newsletters, the issuing of

[1] The following report contains both original research results as well as parts of and the summary of previous research results, the relevance of which was considered important by the project partners in the PEAKapp research project. These earlier research results stem partly from the projects SMARTIES (FFG No. 850106) and RASSA (FFG No. 848811).

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

loyalty cards, video surveillance, webshop activities, social media campaigns, gambling events, the operation of electronic licensing systems, etc.

Energy companies also have a large amount of personal data: Data from electricity and natural gas customers, data from employees, as well as data from third parties such as service providers, suppliers and business partners. This data is subsequently processed: Customers provide their name, date of birth, address, e-mail address and bank account details on registration forms and may use an online customer centre; employee directories and personnel files are maintained and programs are used for billing and customer traffic.

The GDPR entails many changes for companies. Companies in non-EU countries are also affected by the new rules as far as they offer goods or services to EU citizens or observe their behaviour. The mere accessibility of an EU-external website within the EU is not considered such an offer. Profiling and other user tracking on the internet in contrast count as observation of the behaviour of EU citizens.

In addition, so-called flexibility clauses in the GDPR allow EU countries to enact national legislation in specific areas. Germany and Austria have already made use of this right, while in many other countries the EU transposition act is still pending.

Any organisation that does not meet the requirements of the GDPR beginning 25/05/2018 must expect significant sanctions. According to the GDPR, penalties of up to EUR 20 million or 4% of the total worldwide turnover of the previous year can be imposed. It is expected that EU regulators will increase their activities and impose heavy fines, but at the beginning are more likely to be cautions. Private individuals can also file for damages.

As this new regulation is also highly relevant for the energy sector, a rough overview of the GDPR is provided first here. Furthermore, the scope of application is defined, the principles of the GDPR and data subjects' rights are analysed, and an overview of the data protection impact assessment is provided.

Because one of the relevant questions in the project relates to the transfer of energy consumption data when changing residences, this text concludes with a discussion of the newly added right to data transfer pursuant to Art. 20 GDPR.

2. New EU data protection law

The new data protection law brings many changes with it. The energy sector is also affected. The specific features of smart meters raise some important specific questions regarding the application of the GDPR and the planned recasting of the EltRL, such as the definition of "energy data", the allocation of responsibilities for energy management and the rights of data subjects. Digitalisation and the increased use of mobile devices in connection with smart meters and smart homes are also creating new risks. In the following, a rough overview of the new General Data Protection Regulation as well as the relevant provisions of the so-called "Winter Package" will be provided.

The European Commission initiative on the EU data protection reform of January 2012 is now being implemented. In December 2015, the European Parliament and the Council reached an agreement on the Commission's data protection reform. On 8 April 2016, the Council adopted the General Data Protection Regulation (GDPR) and the Data Protection Directive[3]. On 14 April 2016, the Regulation and the Directive were adopted by the European Parliament. [4] On 4 May 2016, the official texts of the Regulation and the Directive were published in the Official Journal of the EU in all official languages. While the Regulation entered into force on 24 May 2016, it has applied since 25 May 2018; the Directive entered into force on 5 May 2016 and the EU Member States were required to implement it nationally by 6 May 2018.

The GDPR is an essential step to strengthen citizens' fundamental rights in the digital age and to facilitate business by simplifying rules for businesses in the digital single market. The Data Protection Directive for Police and Criminal Justice protects the fundamental right of individuals to privacy when personal data is used by law enforcement agencies, which also facilitates cross-border cooperation between EU Member States.

Standardizing data protection requirements is not the only field in which the EU has begun to harmonise various pieces of legislation. Similarly, in the second half of 2016, the European Parliament, the Council and the Commission reached an agreement on the security of

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, and for free movement of such data, as well as the repeal of Council Framework Decision 2008/977/JI of the Council.

[4] *European Commission*, Data protection, ec.europa.eu/info/law/law-topic/data-protection_en (Stand 4. 11. 2017).

network and information systems (NIS Directive [5]). The provisions of the NIS Directive aim to make the online environment more trustworthy thereby supporting the proper functioning of the digital single market in the EU.

The above two legislative initiatives (GDPR and NIS) provide a new framework for data protection and cybersecurity management in the EU in times of continuous digitisation of industry (including the energy sector).

In Europe, data protection law is one of the most important legal instruments when processing and using information about persons.[6] The right to protection of personal data is a fundamental right in the EU[7], and in accordance with Art. 16 (1) of the Treaty on the Functioning of the European Union (TFEU)[8] everyone has the right to protection of their personal data.

Personal data plays a central role in today's society. While the diffusion of technological innovations has made the processing of personal data omnipresent through automated means, enforcement of individual rights has not been in the foreground. The GDPR is not only aimed at strengthening the right of citizens to better control their personal data, but also creates a new legal framework that brings together data protection legislation in the EU Member States.[9]

The Regulation retains the core of the 1995 Data Protection Directive[10] but updates and modernises privacy principles. There is a strong focus on the following points:

- Strengthening the rights of individual persons;
- Strengthening the EU single market;
- Ensuring greater enforcement of legislation;
- Limitation of the international transfer of personal data; and
- Setting global privacy standards.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union.

[6] See Art. 1 and 6 and Recitals 1, 13, 14 GDPR.

[7] Art. 8 (1) Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights of the European Union, 2000/C 364/01.

[8] Treaty on the Functioning of the European Union, 2012/C 326/01.

[9] Recitals 2, 7, 9, 10, 13 GDPR.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of data.

3. Data protection and smart meters: the GDPR and the "Winter Package"

An important innovation through the harmonisation of the Third Energy Package, in particular under the directives for the single market for electricity[11] and gas[12], was the introduction of smart metering systems to support consumers' active participation in the electricity and gas supply markets.

The objective of the Internal Market in Electricity Directive 2009 (EltRL 2009) was clearly to inform consumers about their consumption data. It is clear from the recitals that access to objective and transparent consumption data is a key aspect of supplying customers. The customer should have access to their consumption data and have free access to the data. Only with their express consent and free of charge can the customer also grant suppliers access to this data. However, there is also the possibility that other persons should have access to the consumption data.

Furthermore, Annex I of the EltRL 2009 (heading: "Measures to protect customers") states in its paragraph 2 that Member States shall ensure that smart metering systems are introduced that support the active participation of consumers in the electricity supply market. The introduction of these measuring systems may be subject to an economic evaluation, which will examine all the long-term costs and benefits to the market and to individual consumers. In addition, it is possible to investigate which type of smart measurement is economically justifiable and cost-effective and in what time frame the introduction is practically possible.

On the basis of this assessment, Member States prepare[13] a timeline with a planning goal of 10 years for the introduction of smart metering systems. If the introduction of smart meters is assessed positively, at least 80% of consumers will be equipped with smart metering systems by 2020. Member States, or the competent authorities designated by them, shall ensure the interoperability of the metering systems used in their territory and shall take due account of the application of the relevant standards and best practices, and of the importance attached to the development of the internal electricity market.

[11] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the single market in electricity and repealing of Directive 2003/54/EC, OJ L 211 of 14/08/2009.

[12] Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the single market in natural gas and repealing of Directive 2003/55/EC, OJ L 211 of 14/08/2009.

[13] Or a competent authority designated by them.

A similar legislative provision can be found under the Energy Efficiency Directive (EED)[14], where it is stipulated that customers should have a low-cost single meter for electricity, natural gas, district cooling and hot water. This meter should accurately reflect energy consumption and state the exact time of energy consumption[15]. In addition, the 2012 EED also deals with data protection and security in the installation of smart meters and imposes obligations on Member States to comply with the relevant data protection and data protection rules of the Union.

Smart meters are digital versions of traditional mechanical meters that have two-way communication capacity. They are currently most commonly used for electricity metering, but the principles can also be applied to other utilities. These meters can transmit information directly from the metered unit to the utility, in near real time and with very high granularity of the data.

With smart meters in use across Europe, the amount of data available on energy use is increasing enormously. As mentioned above, the EU data protection framework imposes significant restrictions on the processing of personal data. Since smart grid and smart metering systems inevitably process personal data as part of their routine technical processes and in fact derive added value from that processing, they must be assessed in relation to their EU application from this point of view.

In addition, the Clean Energy Package 2016[16], also known as the "Winter Package", strengthens the role of intelligent metering systems. Among other things, by helping consumers in the centre of the Energy Union to benefit from access to safe, clean and competitive energy. The Commission acknowledged that it was time to update the existing framework to be consistent with the increased level of flexibility and decentralisation of today's energy sector, and to provide a favourable environment for the "paradigm shift" to a more competitive and consumer-oriented market structure[17].

[14] Directive 2012/27/EU of the European Parliament and of the Council of 25/10/2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC , Abl. L 315/2012, 1 (EED 2012).

[15] Art. 9ff EED 2012.

[16] *European Commission*, Proposals on clean energy for all Europeans, ec.europa.eu/commission/priorities/energy-union-and-climate/proposals-clean-energy-all-europeans_en (Stand 29. 11. 2016).

[17] *European Commission*, Commission proposes new rules for consumer centred clean energy transition - Energy - European Commission, ec.europa.eu/energy/en/news/commission-proposes-new-rules-consumer-centred-clean-energy-transition (Stand 25. 11. 2016).

In particular, the proposal for a recast of the EltRL[18] introduced new rights to strengthen and better protect end-users, such as the right to clearer billing information and tools for certified comparisons, the right to a dynamic pricing contracts and the ability to self-generate electricity. Smart meters are the essential tools for effectively exercising these rights. In this context, the proposed recast of the Directive includes specific definitions for smart consumption systems and interoperability and devotes a special section to the functions, provision and management of smart meters in Art. 19 to 24 of the proposal for the new EltRL.

Art. 20 of the proposal for the new EltRL contains seven principles for the introduction of smart meters. Of these seven principles, four relate to the protection of personal data, including the rights of consumers and data subjects. In particular, Art. 20 (b) and (c) leg cit state that the security of data communications and data protection of end users must be ensured in accordance with the relevant Union security and data protection rules. As regards the rights of data subjects, Art. 20 (e) of the proposal for the new Directive states that energy consumers should have access to the metering data for their electricity supply and collection in an easily comprehensible form, while (f) leg cit obliges Member States to ensure that consumers are properly informed at this time of the installation of smart meters and the collection and processing of their personal data.

In addition to the principles set out above, the provisions in Art. 23-24 and Annex III of the proposal for the new EltRL focus on the access and management of energy data. It also reaffirms the need to ensure the highest levels of cybersecurity and data protection through the use of best available techniques.[19]

3.1. ICT system "device application"

Companies are faced with a further challenge comes with the use of mobile devices because they are extremely difficult to monitor.[20]

First, these devices can be taken everywhere, so they are exposed to various attack vectors, for example through other Wi-Fi networks. Second, a large number of people are using their smartphones, tablets and notebooks not only for business but also privately, for example by

[18] Proposal for a Directive of the European Parliament and of the Council establishing common rules for the internal market in electricity, COM(2016) 864 final.

[19] See *Fratini/Pizza*, Data protection and smart meters: the GDPR and the 'winter package' of EU clean energy law, eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html (Stand 14. 6. 2018).

[20] *ZfK*, Studie: Ein Drittel aller deutschen Unternehmen fürchten EU-Datenschutzgrundverordnung, zfk.de/digitalisierung/it/artikel/studie-ein-drittel-aller-deutschen-unternehmen-fuerchten-eu-datenschutzgrundverordnung-2018-02-20/ (Stand 20. 2. 2018).

downloading apps for private use. Finally, mobile devices are often lost. So it is difficult to predict who will get their hands on these devices or where the devices will end up. However, these issues conflict with the rule that company employees must know who has access to the data and how it is processed. In this regard, it is usually not possible for companies to exercise all-encompassing control of such devices here. In addition: If the device is stolen and data is lost or third parties gain access to personal data, companies may need to respond within 72 hours.

The use of apps is always accompanied by legal issues regarding data protection law. Large amounts of data are stored and used with every app use. Data protection law provides for the principle that data collection, data storage and data usage is only permitted with the consent of the data subject. This always concerns personal data such as data involved in the use of apps. The problem with the consent here is that due to the small displays of smartphones, there is a likelihood that hardly anyone reads page-long terms and conditions or privacy policies. Informed consent cannot be easily assumed here.[21] That is, users must agree to data collection, storage, and usage when installing the app, which is what many apps do. According to the new GDPR, users have the right to have data deleted at any time[22].

App development is software development. And the same legal issues arise in this regard. On the advice of *lawyer Thomas Feil* "the contracts that specify the development of an app should maintain a precise list of shortcomings so there are no complications. For example, it should be clarified that the app should always be updated to the latest version of the operating systems for smartphones and tablets. Otherwise, the app quickly becomes unsuitable with the next Android or iOS update and there are complicated liability issues. In addition, it should be clarified to what extent rights of use of the app (copyrights) are granted. When developing the app, developers should ensure that no copyright violations are committed - the graphical elements may not be taken over by third parties without a license, just as little musical elements or texts can."[23]

App users are in a triangle relationship with the distributors and the app provider. For example, Apple is responsible only for the distribution of the app and all related problems

[21] *Feil*, Rechtliches zu Apps und App-Entwicklung, anwalt.de/rechtstipps/rechtliches-zu-apps-und-app-entwicklung_057414.html (Stand 25. 3. 2014).

[22] *Schwenke*, Die rechtlichen Rahmenbedingungen der App-Entwicklung, textintern 2012, 6 (6)6.

[23] *Feil*, Rechtliches zu Apps und App-Entwicklung, anwalt.de/rechtstipps/rechtliches-zu-apps-und-app-entwicklung_057414.html (Stand 25. 3. 2014).

such as transmission errors. In addition, however, the app provider takes over any responsibility for support, warranty and any liability vis-a-vis the app user. Due to this responsibility, it is advisable for the app provider to design their own app terms and conditions in which liability or usage restrictions are agreed. These terms and conditions are often even necessary if liability notices - such as in the use of location-based services - must be accepted obligatorily.[24]

The following also applies for data protection: “Ignorance does not protect you from punishment”. If personal data is illegally collected or used, the app provider, as the responsible data controller, can be fined. The provider of an app is primarily responsible for compliance with data protection regulations even if it has not developed the app itself or uses service providers.[25]

Data protection law is only applicable to personal data. The following information may, for example, allow conclusions to be drawn about a natural person:

- IP address
- Device and card ID (IMEI, UDID, IMSI, MAC address)
- Mobile phone number (MSISDN)
- Name of the phone
- Location data
- Photos, videos
- Audio files
- Biometric data (e.g. fingerprint)
- Usage data
- Contact details
- Calendar items
- Registration data
- Call lists
- Messages
- Account data[26].

[24] *Schwenke,* textintern 2012, 6.6.

[25] *Leissler*, Apps & Datenschutz, ipCompetence 2012 H 8, 46, 46.

[26] *Unverzagt von Have* in Unverzagt von Have Rechtsanwälte Partnerschaftsgesellschaft mbB, Neue Hinweise der Datenschutzbehörden zum Datenschutz im Mobile Bereich | Online-Marketingrecht

Even in the early development phase, the basic principles of data protection should be taken into account. The principle of direct collection is violated, for example, if the basic settings are set so that the phone book of a user is automatically read. In addition, it is necessary, due to the earmarking principle, to determine in advance for the app whether the access rights to data are necessary for the intended purpose[27].

4. Scope of application of the GDPR

The scope of the GDPR can basically be divided into three areas: the material, the personal and the territorial scope. The material scope includes the nature and scope of the data protection rules. The personal scope of application, on the other hand, refers to the persons whose data is to be protected as well as to those who are obliged under the data protection regulations, i.e. those who "process" the data. The territorial scope of application defines the geographical areas in which the GDPR applies.

4.1. Material scope

The material scope of the GDPR covers both the automated processing of personal data and the non-automated, i.e. manual, processing of personal data, if the data is to be stored in a data system.

The material scope covers the "processing" of data. In accordance with Art. 4 (2) of the GDPR, this includes any operation or series of operations carried out with or without the aid of automated procedures in connection with personal data such as collection, gathering, organisation, ordering, storage, adaptation or modification, reading out, querying, using, disclosing through transmission, dissemination, or any other form of provision, reconciliation or association, restriction, erasure or destruction. Accordingly, the transmission of data to the data subject and to the processor is also included[28].

Personal data is defined in Art. 4 (1) GDPR as "any information relating to an identified or identifiable natural person (the 'data subject'); a natural person is considered as being identifiable, directly or indirectly, if this natural person can be identified in particular by means of an identifier such as a name, an identification number, location data, an online identifier or

(Stand 6. 10. 2014, onlinemarketingrecht.de/2014/10/neue-hinweise-der-datenschutzbehorden-zum-datenschutz-im-mobile-bereich/).

[27] *Leissler,* ipCompetence 2012 H 8, 46, 46.

[28] More precisely, see Fritz, "Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? in *Jahnel*, Datenschutzrecht. Jahrbuch 2016[1] (2016) 18.

one or more special characteristics expressing the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person.

Accordingly, basically all information is included, on the basis of which reference can be made to a natural person, i.e. all data that makes a person identifiable. Furthermore, the GDPR specifies which data makes it possible to identify a natural person. In order to determine the identifiability of a natural person, according to Recital 26, all means likely to be used by the controller or another person in their general discretion to identify, directly or indirectly, the natural person, such as sorting, should be taken into account. In order to determine which means are likely to be used with general discretion to identify a natural person, all objective factors should be considered, whereby in Recital 26 examples are provided regarding the cost of identification and the time required for identification. The technology and technological developments available at the time of processing should also be taken into account. The GDPR therefore does not apply to anonymous data; accordingly, it does not apply to personal information that has been anonymised in such a way that the data subject cannot or can no longer be identified. The GDPR therefore does not apply to the processing of anonymous data for statistical or research purposes, although the processing of personal data (in non-anonymised form) for statistical purposes is indeed governed by the GDPR[29].

However, this is different for data that is pseudonymised [30]. In pseudonymisation, the name or another identification feature is replaced by a pseudonym (usually a multi-digit combination of letters or numbers, also called a code) in order to exclude or significantly impede the identification of the data subject. Thus, if personal data is pseudonymised, it could be assigned to a natural person by using additional information, so pseudonymised data is considered to be information about an identifiable natural person and thus subject to the GDPR.

As a special category, Art. 9 (1) of the GDPR includes personal data which allows identification of a natural person regarding racial and ethnic origin, political opinions, religious or ideological beliefs or trade union affiliation, as well as genetic data and biometric data for

[29] See Recital 162 GDPR.

[30] Pursuant to Art. 4 (5), pseudonymisation means the processing of personal data in such a way that personal data can no longer be attributed to a specific data subject without additional information, provided that such additional information is kept separate and subject to technical and organisational measures to ensure that the personal data is not assigned to an identified or identifiable natural person.

the unambiguous identification of a natural person [31], health data, or sex life or sexual orientation data regarding a natural person.

4.1.1. Definition of "energy data"

Smart metering systems process huge amounts of data as part of their routine technical operations. But are all these data personal data?

The answer is clear for registration data provided by the data subject when signing the contract for the introduction of a smart meter. For example, data such as name, address and information about the user's billing information and payment methods are undoubtedly personal data..

"Energy data" of the user is referred to in the planned recast of the EltRL as measurement and consumption data and as the data required for a provider change. While this data might at first glance be considered technical data and thus would not fall within the scope of the GDPR, the data is in fact linked to the natural person, who can be identified by a unique identification number, e.g. a counter identification number. This data should therefore be considered personal data because it relates to an identified or identifiable user and discloses information about their energy consumption, thus providing insights into the daily life of the data subject. If the data subject is a "prosumer", i.e. someone who both consumes and produces electricity, "energy data" refers to the amount of energy fed into the network, which in turn provides information about the amount of available energy resources of the data subject.

This definition of "energy data" as personal data is in line with the GDPR, whose definition of personal data also includes information that discloses the economic situation of the data subject. Energy data can be more or less detailed depending on the needs of the user as it can be designed and customised accordingly. On the one hand, "energy data" is a valuable asset for end users who want to reduce energy consumption and adapt their behaviour to variable tariffs. On the other hand, companies and politicians also have a valuable tool in

[31] According to Art. 4 (14) biometric data is "personal data obtained by means of special technical procedures, regarding the physical, physiological or behavioural characteristics of a natural person, which enable or confirm the unambiguous identification of this natural person, such as facial images or dactyloscopic data.

real-time consumption data to effectively approach, monitor and evaluate energy efficiency measures.[32]

However, smart meter data can also be used for other purposes. Energy data enables better understanding of customer segmentation, customer behaviour, and the impact of pricing on usage. This data can therefore be used for specific profiling exercises, e.g. to collect information about the end user's energy footprint in their private environment, their behaviour habits and preferences. Smart meters also impacts competition in the power markets because the provision of accurate, reliable and up-to-date data flows via smart metering infrastructure allows for easier and faster switching between providers. Access to user data in terms of energy preferences is therefore a major benefit for utilities. For this reason, an adequate level of protection should be ensured during both the transmission and the processing phase in order to avoid unauthorised user profiling based on the detailed meter readings and other possible "further" uses of this data.

If energy data is later combined with data from other sources, such as geo-location data, data available through internet tracking and profiling, video surveillance systems and radio frequency identification (RFID) systems, the potential risks associated with collecting detailed consumption data as part of the so-called "Internet of Things" increases.

In this regard, smart meters could be an entry point to gain privileged access to the digital realm of a household.

In a device application that uses data from a smart meter, the following categories of data are processed:

- App usage data: Data that collects the different interactions of the user with the app and that allows an analysis of the user's use of the app (e.g. session duration, number of bets, ...).
- Customer data: Personal information about the app users, descriptive data about households (e.g. household size, ...). To protect the identity of the app user, this data is anonymised, but it remains in principle personal data.
- Meter data: Smart meter data is data that indicates the household's energy consumption in continuous time intervals (i.e. load profiles). Smart electricity meters collect the consumption data from device owners and store them on the device.

[32] *Fratini/Pizza*, Data protection and smart meters: the GDPR and the 'winter package' of EU clean energy law, eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html (Stand 14. 6. 2018).

Transmission of the data to the network operator then takes place, depending on the system setting, either once a year, monthly, daily or at even smaller intervals. According to Art. 4 (1), the consumption data recorded with the aid of smart metering instruments is covered by the term (personal) “data” within the meaning of the GDPR, since these devices record information on data subjects - namely energy consumption - whose identity is unequivocally determined or can be determined at least via the point of delivery and thus allow conclusions to be drawn about the habits of the data subject.[33] Even if more than one person lives in a household and therefore an immediate attribution of energy consumption to individuals is not possible, personal data is available at least with regard to the subscriber.[34] In a similar sense, the Data Protection Commission[35] has defined phone numbers as personal data of the subscriber, although in this case several people may still use the mobile phone. However, if data from several households, several houses or even entire streets is aggregated, personal data is no longer available and the GDPR is not applicable.

- Contract data: Information about the energy contract between the household and the energy retailer. It provides information on the type of tariff available to the household, the duration of the contract, the contract number and tariff data. Since, for example, the person concerned can be clearly identified by means of the contract number, individual data from this category is also considered personal data.
- Survey data: Field test customers are asked to complete small online surveys sent to them via the app. These surveys serve to better understand what measures interviewees have taken to reduce their energy consumption. To protect the identity of the app user, this data is anonymised.

In principle, it is not clear that in the energy sector data is processed from the special category pursuant to Art. 9 (1) GDPR. However, it would be conceivable to use biometric data in applications for mobile devices, such as for opening the app. In this case, the stricter provisions pursuant to Art. 9 (1) GDPR with regard to this particular category would apply.

[33] For example *Renner*, Smart Metering und Datenschutz in Österreich, In:, Datenschutz und Datensicherheit (DuD), 524 (21) and *Buschmann/Motyka*, Energieeffizienz als Schlüssel zur Klima- und Ressourcenschonung? wbl 2011, 11 (16).

[34] At least the information that someone is the owner of an electricity connection, about the amounts of energy that are purchased at certain times etc.

[35] DSK 09/08/2006, K121.109/0006-DSK/2006.

4.2. Territorial scope

Compared to the "old" data protection law, there are significant changes in this field of application since the GDPR is also applicable to data processing outside the EU if certain conditions are met.

According to Art. 3 (1), the GDPR is applicable to the processing of personal data, irrespective of whether the processing of this data takes place in the EU. It refers to the establishment of a controller or commissioned processor in the Union. Regarding the legal form of the branch it is the same whether it is a branch or a subsidiary with its own legal personhood. The deciding factor is the effective and actual exercise of an activity by a fixed body.[36]

In any case, the GDPR is also applicable if the data processor has a branch in the EU and processes data for a client not established in the EU.

In addition, the GDPR is also applicable if personal data is processed by controllers or commissioned processors without a branch in the Union. It is applicable even if the processing of data for the branch does not take place in the EU at all. Accordingly, the GDPR may also apply if no processing step are taken within the Union. This occurs when personal data of data subjects located in the Union is processed and is related to the offering of goods or services. It does not matter here whether these goods or services are offered against payment or free of charge. In deciding whether the controller or commissioned processor intends to provide the data subject with goods or services in at least one Member State of the Union, factors such as the use of a language or currency common in that country may be included. The mere accessibility of the website of the controller, commissioned processor or mediator in the Union, an e-mail address or other contact details or the use of a language generally used in the third country in which the controller is established, is still not sufficient evidence of the provision of an offer to data subjects within the Union.[37]

The processing of personal data of data subjects by a controller or commissioned processor located outside the Union is also subject to the GDPR if it serves to monitor the behaviour of those data subjects, provided their behaviour takes place in the Union. Such a behavioural observation would be possible, for example, with an analysis tool for internet behaviour. In order to assess whether a processing activity involves the observation of the behaviour of data subjects, it should be determined whether the internet activities of the data subjects are

[36] See Recital 22 GDPR.
[37] See Recital 23 GDPR.

tracked, including the possible subsequent use of personal data processing techniques that profile a natural person which, in particular, provides the basis for decisions relating to them or for analysing or predicting their personal preferences, practices or habits.[38]

This regulation also applies to those responsible for processing personal data in a place which is subject to the law of a Member State under international law.

4.3. Personal scope

With regard to the scope of application, three groups of people are clearly distinguished: The data subject, the controller and the commissioned processor.

4.3.1. The data subject

Pursuant to Art. 1 (1), the GDPR contains regulations for the protection of natural persons. Any natural person, regardless of nationality or whereabouts, may benefit from the protection afforded by the regulation. It follows that nationals of third countries or EU citizens resident in third countries can also rely on the GDPR[39].

Unless member states provide for further regulations, the GDPR does not apply to the personal data of deceased persons. [40]

In any event, this regulation does not apply to the processing of personal data of legal persons and in particular companies founded as a legal entity, including the name, legal form or contact details of the legal person.[41]

4.3.2. Controller and commissioned processor

According to Article 4 (4) of the GDPR, the controller is the natural or legal person, public authority, body or other entity that, alone or in concert with others, decides on the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union law or the law of the Member States, the controller or the specific criteria for its designation may be provided for under Union or national law.

The commissioned processor may also be a natural or legal person, an authority, a body or another entity. The commissioned processor processes the personal data on behalf of the controller.[42]

[38] See Recital 24 GDPR.
[39] If the processing of their personal data also falls within the material and territorial scope of application of the GDPR.
[40] See Recital 27 GDPR.
[41] See Recital 14 GDPR.

While an organisation may have different data protection roles with respect to different processing activities, an organisation may only be either a controller or commissioned processor for a specific processing activity.[43] The central distinction criterion between these two roles is whether the organisation decides on the purposes and means of processing personal data.

Both the controller and the commissioned processor are responsible for the personal data they process. The controller determines the purpose of processing the data while the commissioned processor carries out the actual processing. The commissioned processor decide show the personal data will be stored and what security measures will be used, as well as the selection of IT systems and other methods necessary to collect the data. In addition, the commissioned processor decides how the information provided by the data subjects is taken over and also deleted.

Thus, while the commissioned processor decides on and implements these points, the controller is responsible for collecting the data and determining its legal basis. It determines the purpose of using the data and determines whose and which data is collected.

The commissioned processor now also has direct obligations under the GDPR. This includes the obligation to maintain a register of all processing activities carried out on behalf of a controller and, if necessary, to designate a data protection officer[44] and to assist controllers in complying with the reporting obligations. Provisions on cross-border transfers also apply to commissioned processors, and binding corporate rules for commissioned processors are formally recognised. The new status of data processors is likely to affect how data protection matters are regulated in supply and other trade agreements.

In summary, the tasks of the commissioned processor and the controller are as follows:

<u>Obligations of the commissioned processor</u>

- The commissioned processor must implement all data security measures of the GDPR. This includes, among other things, the pseudonymisation and encryption of personal data as well as ensuring the confidentiality, availability and resilience of the systems and services related to the processing.

[42] See Art. 4 (8) GDPR.

[43] *Article 29 Working Party*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und Auftragsverarbeiter“ (Stand 22. 6. 2018).

[44] As well as the appointment of a representative (if the data protection officer is not based in the EU).

- Each commissioned processor shall keep a record of all processing activities carried out on behalf of a controller.
- It is obliged to cooperate with the supervisory authority on request.
- The commissioned processor must perform risk analyses of the data applications and assist the controller in the performance of its duties under the GDPR.

Duties of the controller

- The controller must take appropriate technical and organisational measures into account in both planning and data processing in order to ensure adequate protection for the respective risk.
- The controller must also take appropriate technical and organisational measures to ensure that, through appropriate defaults, only that personal data is processed whose processing is required for the particular processing purpose.
- The controller must keep a record of all processing activities within its responsibility.
- The controller must document all violations of the protection of personal data, including all facts in connection therewith (impact, remediation).
- The controller is required to conduct its own evaluation of data processing in order to analyse the implications and risks of data processing regarding the data subjects' rights and to estimate the consequences for data protection. This "self-evaluation" is called a data protection impact assessment[45] in the GDPR.

For both the commissioned processor and the controller, it is obligatory to appoint a data protection officer as soon as the conditions are met pursuant to Art. 37 (1) GDPR.

4.4. Data management and assignment of responsibilities

As clearly stated in Art. 23 of the planned recast of the EltRL on data exchange and management in connection with the introduction of smart meters, all issues related to the processing of energy data should be resolved at the national level. It follows that Member States or competent authorities organise data management to ensure efficient data access and exchange. This process also includes the identification of the authorised parties who may have access to the data of the end customer, provided that express consent has been granted in accordance with the provisions of the GDPR. Authorised parties shall at least include customers, suppliers, transmission and distribution system operators, aggregators, energy service companies and other parties providing customers with energy or other

[45] For details, see Chapter 7.

services. This list is not exhaustive given the highly dynamic environment of the energy sector.

As explained above, the GDPR defines the characteristics and responsibilities of controllers[46], commissioned processors [47] and third parties who collect and process personal data. The controller, alone or in concert with others, is responsible for defining the purposes and means of processing personal data, while the commissioned processor carries out the processing of personal data on behalf of the controller.[48] The third party processes personal data under the direct supervision of the controller or the commissioned processor and only if authorised to do so by the latter. Finally, the recipient is the party to whom the personal data is disclosed, whether or not it is a third party.

Since the introduction of smart meters involves a number of actors in the processing of personal data, it is important to identify who in this context should be considered as a data controller, commissioned processor or simply an authorised third party. The allocation of roles and responsibilities may not be clear, as the arrangements for the deployment of smart metering - and hence the data management model - need to be regulated at Member State level and there are no clear guidelines at EU level. Given the number and complexity of relationships, applying the relevant definitions is not easy.

However, the following roles and responsibilities can be identified on the basis of the GDPR. The controller could be the person responsible for the measurement and consumption data, the contractual data and the network data. The mission of the controller is to collect, validate, analyse and archive historical data, to ensure that customers have access to their consumption data and have access to their metrics through explicit consent and free registration.

The role of the commissioned processor could fall to the person who collects or aggregates the measurement and consumption data. The commissioned processor is responsible for reading the meter reading and the quality control of the data.

In the planned recast of the EltRL, to ensure compliance with data protection requirements, it is proposed that those parties managing the data be authorised and certified by the competent national authorities. In any event, this regulation is consistent with the GDPR, which requires Member States to introduce certification mechanisms and codes of conduct in

[46] See Art. 4 (7) GDPR.
[47] See Art. 4 (8) GDPR.
[48] See Chapter 4.3.2.

order to demonstrate that the controllers or the commissioned processor have taken appropriate security measures.

In most Member States, the distribution system operator is responsible for measuring and is the data controller in the first phase of the measurement data process. The traditional distribution operator process ends with the creation of a network usage bill. In a second step, the measurement data is forwarded to the electricity supplier, who is responsible for the billing and supply of the consumers and thus acts as a commissioned processor in this final phase of the processing. In principle, distribution system operators are already involved in the processing of personal data, as they have detailed information about the status of network components, about generators connected to the network, and about energy flows throughout the network. In some cases, the distribution system operator outsources parts of its metering to a meter operator. This is a facility that provides services related to the installation, maintenance and operation of metering equipment related to supply. This role could be further divided into two units, one responsible for managing the meter and the other for managing meter data. In this event, the metering point operator assumes the role of the commissioned processor due to a contractual agreement with the distribution system operator. However, in most Member States metering is considered part of the "distribution" business, with the distribution system operator both owning and being responsible for the introduction of smart meters and access to metering data.[49]

Despite the leading role of distribution system operators in the management of smart meter data, some Member States have[50] decided on a separate entity (central communication hub) that provides third party access to metrics and decouples the processing of data from the physical meter. In such a system, the data of the consumers is stored on the smart meters installed in their premises, and the central node unit is responsible for forwarding (but not storing) data, collecting it from the devices in the premises of the consumer and delivering the data to energy suppliers, distribution system operators and other third parties.[51] Such a transfer may be made in accordance with the GDPR if the data subject agrees accordingly.

[49] *Fratini/Pizza*, Data protection and smart meters: the GDPR and the 'winter package' of EU clean energy law, eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html (Stand 14. 6. 2018).

[50] As in the UK

[51] *Mengi/Waechter/Koch*, 500 kHz G3-PLC access technology for the roll-outs in Germany, 18th IEEE International Symposium on Power Line Communications and Its Applications (3/30/2014 - 4/2/2014) 179.

A similar allocation could apply in those Member States that have instead established a communication structure based on a "middleman" (such as a data aggregator) in medium-voltage/low-voltage substations, which acts as a communication gateway between the data management system and the smart meters. The data aggregator often collects information and data from multiple meters in a specific geographic area before sending the data to a central database for billing, troubleshooting, and analysis.[52] Aggregators are heavily used in densely populated areas.

5. The main processing activities of each actor in the energy sector

5.1. Suppliers

The following chapters provide an overview of the main processing activities of an energy supply company.

Suppliers of energy are responsible for supplying consumers with energy. They source this energy from their own sources and/or the wholesale market and charge it to consumers.

The electricity market was liberalised in 2001. Liberalisation has separated the network and supply sectors. The task of the network operator is the construction, expansion, maintenance and operation of the power grid and the guarantee of a secure power supply in its designated network area. The responsibility of the network operator is determined by the location of the customer. In contrast to the network operator, which is always the same for each location, energy suppliers are in free competition. Customers thus have the opportunity to choose their energy supplier freely on the market and to switch them while the network operator remains the same. By separating the areas of network and supply, the customer concludes a network access contract with the distribution system operator and a delivery contract with the supplier on the basis of officially approved general conditions and government-defined tariffs.[53]

The example of Austria

[52] *Shiobara/Palensky/Nishi*, Effective metering data aggregation for smart grid communication infrastructure, in *Ohishi/Hashimoto* (Hrsg), IECON 2015 - Yokohama (2015) 2136.

[53] *Austria's Energy*, General information on the change of supplier <http://oesterreichsenergie.at/lieferantenwechsel.html> ; *Energy-Control Austria*, information on the change of supplier <https://www.e- control.at/industrie/strom/lieferantenwechsel> , Due to the liberalisation of the gas market, the comments also apply to the gas sector.

In 2014, E-Control, as the regulatory authority, passed the Change Ordinance (Wechselverordnung 2014, WVO 2014)[54]. Among other things, this ordinance regulates the process of a change in supplier. If a customer wants to change the supplier, they turn to the desired supplier, fill in the contract form for the new supplier and give them a power of attorney to carry out all necessary steps for the change. Through the exchange platform, the new supplier informs others that it has the customer's authorisation. Before the actual change, the new supplier can perform a search query for metering point and end user identification at the network operator and a binding and notice period query and query the termination dates at the current supplier. The actual change is to be carried out by the network operator. This is initiated by the new supplier at the network operator. The network operator checks whether the point of delivery name and last name or company name specified by the new supplier correspond to the data available to it. If the data match and the change does not overlap with other procedures (registration, deregistration, actual change), the network operator immediately sends change information to the new and the current supplier. The current supplier can object to the actual change and has to submit it to the new supplier and the network operator. If the new supplier insists on the change and sends confirmation of the change date to the current supplier and the network operator, the network operator has to confirm and fix the change date; otherwise, the actual change is terminated by the network operator. The customer will be informed by the new supplier about the change date, their contact details and the authorisation to announce the meter reading to the network operator or the supplier. The supplier has to transmit the meter reading to the network operator via the exchange platform who in turn transmits the consumption data for the final billing to the old supplier.[55] As part of the supplier change numerous personal data is processed and transmitted via the exchange platform between network operators, new and old suppliers. Further transmissions of numerous personal data of the customer between the supplier and the network operator take place at the time of registration as well as deregistration.[56]

Further processing activities of energy suppliers include the management of data of existing customers as well as plant and consumption data. In order to attract new customers, proprietary or purchased customer and prospect data can be used for business initiation regarding the supplier's own service offer. In this data application, customer care and

[54] E-Control ordinance on the change, registration, deregistration and objection (WVO 2014) BGBl II 167/2014.
[55] Appendix to WVO 2014, BGBl II 167/2014.
[56] See also § 76 ElWOG

marketing for own purposes, a distinction is made between different groups of persons: own customers, interested parties who have approached the energy suppliers themselves, and potential interested parties whose addresses were purchased from address publishers or secured by the supplier.[57]

Given the fact that nowadays matters of almost all areas of life can be done via the internet and online, many energy suppliers also provide their customers with an online customer centre. Energy issues such as receiving online invoices, entering meter readings, changing master data or redeeming bonuses can be done conveniently from home.[58] In these online services data on the person of the customer, bank details, billing data and meter reading data such as meter number, meter reading state is processed.[59]

5.2. Distribution system operators

Distribution system operators are responsible for power distribution in high-voltage (generally below 60 kV), medium-voltage (usually between 1 kV and 30 kV) and low-voltage networks.

The term distribution system operator is defined in Art. 2 (6) of the EltRL 2009 as “a natural or legal person responsible for the operation, maintenance, and, if necessary, development of the distribution system in a particular area and, where appropriate, interconnections with other networks. In addition, they should ensure the long-term ability of the system to meet a reasonable demand for transmission of electricity.

In most European markets, the role of a distribution system operator is to be the data centre for measurement data. This role is expanded to include the task of managing an active power network that interacts with the renewable energy source and decentralised generation.[60]

Distribution system operators are involved in the processing of personal data from smart grids or smart metering for the following reasons:

- Distribution system operators receive detailed information about the status of network components, generators connected to the grid, and energy flows

[57] SA0022 Customer service and marketing for own purposes, standard and model ordinance 2014.

[58] Energie Burgenland AG, Online Customer Centre: <https://kundencenter.energieburgenland.at/okc-energie/static.xhtml?id=1522&dswid=- 6811>.

[59] *Data protection authority*, notification of the data application “Online customer centre” of Burgenland Vertrieb GmbH & Co KG, DVR number 1077040, DAN number 1077040/006, 30/11/2016.

[60] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018).

throughout the network. This includes secure remote meter reading to obtain information for network management and supply chain quality. This information should be shared if it is necessary to fulfil regulated tasks of service providers, such as distributed generators or aggregators.

- To avoid network bottlenecks, local load management can reduce the impact on higher voltage levels. Local load management can also be used to improve (local) demand response requests in the case of relatively large uncontrollable distributed generators. Based on their ICT systems for active network management and automatic meter reading, distribution system operators are recommended to further develop these capabilities.

- With the proliferation of conventional distributed generation and the future self-supply generation, the distribution system operator role will gradually shift from the distribution of high-level power supply to the lower levels, while maintaining voltage quality and balance is of key importance because the current now flows in both directions. [61]

The actual implementation depends on the national market model, which provides a central role for the distribution system model in most Member States.
Of course, the supplier change described above also involves, from the point of view of the distribution system operator, a processing of personal data. Furthermore, due to the fact that the customer concludes separate contracts with the network operator, there are online customer centres for network customers for regular customer management, bill viewing, meter readings and registering with and deregistering from the power and gas system. [62]

In the energy sector, the types of data collection and the amount of data, such as in the context of consumption measurement, are also changing. In April 2012, the Smart Meter Implementation Ordinance (IME-VO) was also implemented in Austria[63] for the introduction of intelligent measuring devices (so-called "*smart meters*").

[61] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018)

[62] *Data protection authority*, notification of the data application "Online customer centre" of Netz Burgenland GmbH, DVR number 1074059, DAN number 1074059/012, 1/2/17.

[63] Ordinance of the Federal Minister for Economic Affairs, Family and Youth, which determines the introduction of intelligent measuring devices (Smart Meter Implementation Ordinance - IME-VO), BGBl II 138/2012.

The example of Austria

As stated above, numerous EU directives promote the installation of smart meters that are an integral part of a smart grid[64], especially due to economic considerations.[65]

According to Art. 2 (28) EnEff-RL 2012, an "intelligent consumption metering system" refers to an electronic system for measuring energy consumption, whereby more information is displayed than with a conventional meter[66] and transmission and receiving of data occurs along an electronic communication path.[67] The ElWOG 2010 defines the "intelligent measuring device" as a technical device, which measures the actual energy consumption and usage period in a timely manner and has remote-readable, bi-directional data transmission.[68] With the installation of these new electricity meters, on the one hand, the read-out of the electricity consumption data by the network operator on site, that is to say with the network user, is unnecessary because the meter readings are now read remotely. On the other hand, network users are informed promptly about their actual energy consumption and the associated costs. This should encourage them to control, adapt or reduce their consumption behaviour, especially since they also receive direct feedback on the effects of their behavioural changes.[69] In addition, network users should also be able to request other suppliers to make an offer based on their electricity consumption data. In order to promote energy efficiency, the electricity companies are, according to Art. 3 (11) EltRL 2009, obliged to optimise their electricity consumption through innovative price models. This may include, for example, time-of-use-specific tariffs, tariff rates in critical peak periods, real-time tariffs and peak-time discounts. The same applies to retail rates.[70] But even with these new types of tariffs, consumers need to be informed clearly about current prices and actual energy consumption.[71] Such tariffs, however, for example, that have a negative effect on energy efficiency or can prevent participation in load control pursuant to Art. 15 (4) EnEff-RL 2012 should be eliminated by the Member States.

[64] Without smart grids and smart metering systems, there will be stagnation in renewable energy production and network security is jeopardised, according to a communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Smart Grids: From Innovation to Realisation, COM (2011) 202 final.

[65] For example, in Recital 55 and Art. 3 (11) of the EltRL 2009.

[66] The meter in the default setting shows only the current meter reading. However, display areas can be unlocked at the request of the customer.

[67] Art. 2 (28) EnEff-RL 2012.

[68] § 7 (1) (31) ElWOG 2010 (basic provision).

[69] Recital 50 EltRL 2009; Recital 44 EnEff-RL 2012.

[70] Annex XI Z 3 EnEff-RL 2012.

[71] Annex I (1) (c) EltRL 2009.

Because in the context of the EltRL 2009[72], implementation of the cost/benefit analysis with regard to the introduction of smart meters in Austria has been positive[73], the Austrian legislature has decided on the basis of the authorisation of § 83 (1) ElWOG 2010 that according to § 1 (1) IME-VO [74] every network operator[75]

- must present by the end of 2015 a project plan for the phased introduction of smart meters, including a target achievement path, and
- by the end of 2020 min. 80% and,
- within the scope of technical feasibility, by the end of 2022 min. 95% of metering points connected to its network must be equipped with smart metering devices.[76] Austria has thus gone beyond the requirements of EU law, which has a requirement of min. 80% of consumers by 2020. [77] According to § 1 (5) of the IME Regulation, it is up to the network operator to decide which end consumers it equips with smart metering devices.

In contrast to the conventional, purely analogue Ferraris counter, which merely sums and displays the energy consumption, a smart meter is equipped with the following additional functions:

- Bidirectional data transmission,
- Acquisition and storage of the counts in short measurement intervals,
- Possibility of remote reading and remote shutdown,
- Possibility of offering several tariffs,
- Measuring of energy that is imported and exported e.g. from photovoltaic systems,

[72] Annex I para. 2 of the EltRL 2009.

[73] Art. 9 (1) EnEff-RL 2012 also makes the provision of smart meters subject to the condition of financial viability.

[74] Ordinance of the Federal Ministry for Economic Affairs, Family and Youth, which determines the delivery of intelligent measuring devices (Smart Meter Implementation Ordinance - IME-VO), BGBl. II 138/2012 as amended by the BGBL. II 383/2017.

[75] § 7 (1) (51) ElWOG 2010 (basic provision).

[76] Exempted from this obligation are end consumers whose consumption is measured by means of a load profile counter, § 1 (3) IME-VO.

[77] Annex I para. 2 of the EltRL 2009.

- Communication interfaces for external applications (e.g. household appliances).[78]

The basic provisions are contained in ElWOG 2010. The minimum functional requirements smart meters must meet are defined by the Smart Meter Requirements Ordinance 2011 (IMA-VO 2011)[79]. The Data Format and Consumption Information Presentation Regulation 2012 (DAVID-VO 2012)[80] defines the requirements for the transmission of data from network operator to supplier and consumption information to the end customer.
Consumption values, whether read from the local Ferraris counter or recorded and stored by smart meter, are assigned to a metering point. This concerns information about the consumption behaviour for energy. The assignment of the values to the respective connection owner means this is personal data.[81]

Thus, the annual meter read by the Ferraris meter and the resulting consumption value are personal data that must be used in accordance with the provisions of the GDPR. In recent years, however, the main focus has been on the use of smart meters, as consumption figures are recorded once a day and even every 15 minutes instead of once a year.

According to § 84 (1) ElWOG 2010, the grid operator must record a consumption value once a day and all quarter-hourly values in the intelligent meter starting no later than six calendar months from the date of installation of the intelligent meter and store this data in the smart meter for 60 calendar days for purposes of billing, customer information[82], energy efficiency, energy statistics and maintaining safe and efficient network operation.
Furthermore, according to Art. 84 (2) ElWOG 2010, the network operator is required to read the daily consumption values and, upon express request according to the contractual agreement or consent, quarter-hourly values and make them available free of charge to the end user via a customer-friendly web portal no later than twelve hours after the read-out. By the fifth of the following calendar month at the latest, the network operator must transmit all

[78] *PwC Österreich*, Studie zur Analyse der Kosten-Nutzen einer österreichweiten Einführung von Smart Metering, e-control.at/documents/20903/-/-/cf11cc28-2826-4bf8-95e1-59ba8c75dac3 (abgefragt am 13. 6. 2018).

[79] E-Control ordinance, with which the requirements for smart metering devices are determined (Intelligent Metering Requirements Ordinance 2011 - IMA-VO 2011), BGBl II 339/2011.

[80] Ordinance of the Executive Board of E-Control, which defines the requirements for data transmission from network operator to supplier and consumption information to end customers (Data Format and Consumption Information Presentation Regulation 2012 - DAVID-VO 2012), Federal Law Gazette II 313/2012.

[81] *Schrott*, Einführung intelligenter Messgeräte („Smart Meter“) im Zusammenhang mit Datenschutz und Datensicherheit, in *Jahnel*, Datenschutzrecht. Jahrbuch 2014[1] (2014) 163 (171).

[82] See § 81a ElWOG 2010.

daily consumption data to the respective suppliers for the purpose of consumption and electricity cost information and for purposes of offsetting. Quarter-hourly values may only be transmitted to the supplier after express consent of the end user or for the fulfilment of contractual obligations.[83]

In the context of smart metering, therefore, there is a large amount of personal data processed by the network operator on the one hand and the supplier on the other hand. The reading/capturing, storage, read-out and transmission of the data to the energy supplier are processes of the network operator, and the network operator is data controller. Energy suppliers receive from the network operator the collected consumption data for billing purposes and for the purpose of electricity consumption information, and they are data controllers with respect to these processing operations. [84]

Smart meters offer the advantage of regular and timely consumption monitoring, but also carry the risk that conclusions about the consumption behaviour can be made and the end user becomes a "transparent customer". There is also the risk of hacker attacks and data security manipulations. It could also be a negative for the end customer that the metering devices can be switched off remotely and that the purchase, installation and operation result in high costs.[85]

Not only are meters becoming smart, it is also possible to network the entire home with itself and with the outside world. For example, in a so-called smart home, radiator thermostats and ventilation in living areas, windows, doors, blinds and lamps can be controlled automatically or manually via smartphone or web interface. The total power consumption and power consumption of individual devices can be displayed in an app or web interface. This data can be used in a further step for energy consulting.[86]

A Geographic Information System (GIS) represents another possible processing activity. Information about electricity and gas pipelines is collected, evaluated and visualised here. In addition, basic geographic information such as digital cadastral maps and natural resource

[83] § 84a (2) ElWOG 2010.

[84] *Schrott* in *Jahnel*, Datenschutzrecht. Jahrbuch 14, 163 (172).

[85] *Schrott* in *Jahnel*, Datenschutzrecht. Yearbook 14 163 (164, 165).

[86] *Gabler Wirtschaftslexikon*, Definition Smart Home.
<http://wirtschaftslexikon.gabler.de/Definition/smart-home.html> ; Duden, Definition Smart Home <http://www.duden.de/rechtschreibung/Smarthome>; Data Protection Authority, notification of the data application "VERBUND-ECO-Home" of VERBUND AG, DVR-Number 0040771, DAN-Number 0040771/020, 20/11/2015; Data Protection Authority, notification of the data application "Smart Home" of Wien Energie Vertriebs GmbH & Co. KG, DVR number 2108672, DAN number 2108672/010, 10/10/2014.

data is kept. These processing activities are for the purpose of planning, operation and marketing, calculation of pipeline networks, derivation of maintenance strategies and related data backups and archiving. In addition, with the help of the GIS, line inquiries can be made to third parties.[87] Some energy supply companies offer line information over the internet. In this case, personal data is processed about persons and organisations that request information about routed lines or make an enquiry. In addition to the information about the person, line data, plan and user access data is processed.[88]

Network operators have set up emergency numbers for the purposes of electricity and gas supply. The telephone calls are recorded and stored here. This is done for verifiability, traceability, logging and preservation of evidence. The call recording takes place only with certain, particularly marked apparatuses. Furthermore, attention is drawn to the recording before it occurs. Affected groups of people include the staff of the network operator as well as the emergency-number caller. The date, time and duration of the call, the call content, the extension number, the name of the employee, the caller name and the port number are stored.[89]

5.3. Transmission system operators

Transmission system operators manage the extra-high voltage grid, such as 400 kilovolts (kV) or 225 kV.

A transmission system operator is defined in Art. 2 (4) of the ElRL 2009 as a natural or legal person responsible for the operation, maintenance and, if necessary, development of the transmission system in a given area and interconnections with other networks. In addition, they should ensure the long-term ability of the system to meet a reasonable demand for transmission of electricity.

In order to ensure non-discriminatory access, ownership of the transmission system is separate from electricity trading and generation. High-voltage grids connect all regional

[87] *Data Protection* Authority, notification of the data application "Geographic Information System (GIS)" of Salzburg Netz GmbH, DVR number 4008744, DAN number 4008744/004, 17/11/2015.

[88] *Data Protection Authority*, notification of the data application "line information over internet" of Energie Graz GmbH & Co KG, DVR number 3000283, DAN number 3000283/010, 02/02/2017; Netz Oberösterreich GmbH, online line information. <http://strom.netzgmbh.at/eag_at/page/284094835607631929_0_91656324596202326 3,de.html> .

[89] *Data Protection Authority*, notification of the data application "call recording" of Netz Burgenland GmbH, DVR number 1074059, DAN number 1074059/011, 15/02/2016; Data Protection Authority, notification of the data application "telephone recording" of Wiener Netze GmbH, DVR number 0992704, DAN number 0992704/062, 25/08/2016.

power grids with each other and with the European power grid. In addition to the management of the high-voltage grid, transmission system operators also monitor the reliability and continuity of national electricity trading. Therefore, the transmission system operator is responsible for any correction in the supply and demand imbalance in the electrical energy system. The transmission system operator must use this balancing energy or buy the balancing energy from the balancing energy provider in the event of a bottleneck or surplus of electricity in the system.

The transmission system operators have no relation to the end customer and do not process end-customer data. In the future "smart meter age", they will receive the completely anonymised load profiles daily for all delivery points from all distribution networks in their network area [90].

5.4. Energy generators (producer)

Today, large power plants are responsible for delivering the largest load share. In addition, they are responsible for the delivery of "auxiliary services" such as frequency control, voltage regulation, restart and reserve capacity. This role will generally not change, but with decentralised generation increasing, these decentralised producers will also have to be responsible for grid stability and operational safety.

The move to decentralized energy generation has many benefits, including the use of local energy sources, increased local energy security, shorter transport routes and lower energy transmission losses. Ideally, such decentralisation can foster the development and cohesion of communities by providing sources of income and creating jobs locally.

In a smart grid environment, it is expected that distributed power generators will have access to the data consumption of neighbouring consumers in order to achieve better voltage quality by adjusting production to the consumption of the neighbour, in which case energy generators will be included in the processing personal data from smart meters.[91]

[90] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018).

[91] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018).

5.5. Meter operators

A meter operator is the company that provides services for the installation, maintenance and operation of meters for supply. This role can be divided into two entities as mentioned above: on the one hand the responsibility for the measuring device, and on the other hand the responsibility for the administration of the measured data. In most EU Member States, the distribution system operator is also the meter operator. In contrast to this, for example, in Germany, networks in which several network operators collectively hold a meter operating company are formed. Previously, the meter operator also organised the reading and recording of the meter results.

Meter operators are involved in the processing of personal data from smart grids or smart metering for the following reasons:

- Energy suppliers or independent companies may be responsible for reading meters and managing the metering infrastructure used.
- Meter operators and energy suppliers must (with the consent of the consumer) obtain information on consumption through the metering infrastructure in order to provide this data to other market participants.
- Decentralised producers can collect data on the generated and delivered energy for the grid via the smart metering infrastructure.

In the future of smart metering, the meter operator will no longer receive any meter results. Its customer contact will then be limited mainly to meter exchange and, if necessary, repair.[92]

5.6. Energy service companies

Energy service companies provide energy-related services, such as information or advice on energy saving, energy storage, energy infrastructure outsourcing, energy generation and energy supply, and risk management.

Energy service companies are defined in Art. 2 Z 24 EnEff-RL 2012 as “a natural or legal person providing energy services or other energy efficiency measures in the premises or facilities of an end user”.

[92] *Stiftung Datenschutz*, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/studie-datenportabilitaet.pdf (abgefragt am 1. 6. 2018).

Energy service companies are involved in the processing of personal data from smart grids. The access to and processing of consumer data is usually based on consent or contractual agreement.

Interim results

In summary, the processing of personal data takes place predominantly at the supplier. Therefore, the energy supplier is in most cases the main contact for the consumer. For this reason, the following chapter focuses on the example of the energy supplier.

6. Principles and lawfulness of processing

6.1. Principles of data processing - Art. 5 GDPR

If there is a material and territorial scope, any data processing must comply with the general principles of the GDPR. Pursuant to Art. 5 GDPR, the important key points in the centre of the GDPR are seven general principles for legally compliant storage and processing of personal data.

6.1.1. Legality, good faith, transparency pursuant to Art. 5 (1) (a) GDPR

Personal data will be lawfully processed in good faith and in a manner that is understandable to the data subject. This requires that all information and notifications for the processing of personal data are easily accessible and understandable in clear and simple language. The principle applies in particular to information on the identity of the controller and the purposes of the processing, as well as information about the processing of personal data concerning the data subject.

6.1.2. Purpose-based processing pursuant to Art. 5 (1) (b) GDPR

Personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a way that is incompatible with those purposes. Further processing for archival purposes in the public interest, for scientific or historical purposes or for statistical purposes is not deemed incompatible.

6.1.3. Data minimisation pursuant to Art. 5 (1) (c) GDPR

Personal data must be handled sparingly. Personal data must be appropriate and relevant to the purpose and scope required for processing. This also means that controllers must ensure

through technical preselection that only personal data that is necessary for the respective purpose is processed.[93]

6.1.4. Correctness pursuant to Art. 5 (1) (d) GDPR

Personal data must be factually correct and up-to-date if necessary. All reasonable steps must be taken to remove or correct incorrect personal information.

6.1.5. Storage limitation pursuant to Art. 5 (1) (e) GDPR

Personal data may only be kept as personal data for as long as it is necessary for the purposes for which it was collected. This requires in particular that the storage period for personal data is limited to the absolutely necessary minimum. Therefore, the controller should specify time limits for deletion or periodic reviews. Longer-term storage is permitted after appropriate technical and organisational measures have been taken, for archival purposes of public interest only or for scientific and historical research purposes or for statistical purposes.[94]

6.1.6. Integrity and confidentiality pursuant to Art. 5 (1) (f) GDPR

The principle of data integrity and confidentiality requires that appropriate technical and organisational data security measures be taken. Personal data must be processed in such a way as to ensure adequate security of personal data. Appropriate technical and organisational measures should also ensure that unauthorised persons have no access to the data and that neither the data nor the devices with which they are processed can be used.[95]

6.2. Lawfulness of data processing - Art. 6 GDPR

The processing of personal data requires in any case a legal basis in accordance with Art. Art. 6 (1) GDPR. According to the GDPR, primarily the following possibilities exist as a legal basis:

- The data processing takes place on the basis of a contractual legal relationship or is necessary for the implementation of pre-contractual measures at the request of the data subject;
- There is a legal obligation on the part of the data subject regarding data processing;

[93] *Kastelitz*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 5-11 DSGVO), in *Knyrim* (Hrsg), Datenschutzrecht[3] (2015) 99 (103).
[94] *Fellner*, Betroffenenrechte nach der DSGVO, VbR 2018/47, 84 (85).
[95] *Kastelitz* in *Knyrim*[3] 104.

- The data processing is necessary to protect the vital interests of the data subject or another natural person;
- The processing of data is necessary for the performance of a task which is in the public interest or in the exercise of official authority;
- The data processing is necessary to protect the legitimate interests of the controller or a third party [96];
- There is consent on the part of the data subject for one or more specific purposes of the data processing.[97].

6.2.1. Consent

Consent is a legitimate basis for the transfer of personal data under the GDPR. The definition of consent has changed significantly compared to the previous directive. In cases where Directive 95/46/EC allowed the controller under certain circumstances to rely on an "opt-out" agreement, GDPR now requires that the data subject signal consent with a clear confirming action. The regulation removes the opt-out consent and sets three additional requirements.[98]

First of all, data subjects have the opportunity to revoke their consent as easily as possible at any time. According to Recital 43, the GDPR states that consent is not given voluntarily if there is a clear imbalance between the data subject and the controller, in particular if the controller is an authority. Under Art. 7, an application for consent to data processing must be "clearly distinguishable" from all other matters in a written document and must be made available "in clear and simple language". This means that the consent must be specific to each data processing operation. However, the controller does not have to obtain additional consent if the further processing operations are "compatible" with the original purpose. The meaning of the term "compatible" is explained in more detail in Recital 50. According to Recital 50, interpreting the meaning of "compatible" transactions must, inter alia, take into account:

- Any link between the original purpose and the purposes of the intended further processing;

[96] See Art. 17 (1) (c), Art. 18 (1) (d), Art. 22 (2) (b).
[97] Vgl. *Kastelitz* in *Knyrim*[3] 105f.
[98] *Dürager/Kotschy*, Neuerungen zur Zustimmung (Einwilligung) nach der DS-GVO (abgefragt am 21. 6. 2018).

- The context in which the personal data was collected, in particular the reasonable expectations of the data subjects as a result of their relationship with the controller with regard to the further use of the data;
- The type of personal data;
- The consequences of intended processing for data subjects; and
- The existence of adequate guarantees for both the original and intended further processing.

The new regulation aims to improve the conditions for consent and to make it easier for the data subjects to understand. Accordingly, declarations of consent must no longer be long and illegible, but must be presented in an understandable and easily accessible form. The consent of the data subject to the processing of their personal data must be as simple as possible. In addition, the consent must be decidedly made for the respective purpose of the data processing. Therefore, a separate consent by the data subject is required for each purpose of the data processing.

The following prerequisites are required for a declaration of consent:

- Consent in the form of a declaration or other "unambiguous confirmatory act";
- The information/request for consent must be in understandable and easily accessible form and in plain and clear language;
- The declaration of consent must be clearly distinguished from other provisions (such as terms and conditions);
- Information obligations pursuant to Art. 13ff must be fulfilled;
- The explanation regarding the right of revocation of consent must have taken place before the consent was given; the revocation itself must be as simple as the declaration of consent;
- Each different processing operation requires its own consent unless the other processing operations are "compatible" with the original purpose[99].

6.2.2. Legitimate interest in processing

According to Recital 47 GDPR, the lawfulness of the processing may be justified by the legitimate interests of a controller provided that the interests or fundamental rights and freedoms of the data subject do not prevail. A legitimate interest exists, for example, if there

[99] *Kastelitz* in *Knyrim*[3] 111.

is a customer relationship between the data subject and the controller. In any case, the existence of a legitimate interest must be carefully considered. Accordingly, it should also be examined whether it was foreseeable for a data subject at the time the personal data was collected that processing for that purpose could occur. If the processing of personal data occurs in such a situation that the data subject would not reasonably have been expected to anticipate, the interests and fundamental rights of the data subject could outweigh the interests of the controller.[100]

6.2.3. Further processing

Without prejudice to the compatibility of the purposes of the processing, further processing is permitted only if:

- Consent exists, or
- a legal basis provides for further processing.

In all other cases, further processing must be compatible with the purposes for which the personal data was originally collected. To determine this compatibility, the following should be considered:

- Any connection between the original and the new intended purposes;
- The context in which the data was collected;
- The type of data (in particular whether sensitive or criminally relevant data is present);
- Possible consequences of further processing for data subjects;
- The existence of reasonable guarantees (e.g. pseudonymisation).

If such compatibility with the original purpose exists, no separate legal basis is required other than that for the collection of personal data.

Further processing for public archival purposes, for scientific or historical research purposes or for statistical purposes is considered to be compatible and lawful processing[101].

If the controller intends to process the personal data for another purpose, it must inform the data subject prior to this further processing about this other purpose and all other relevant information.[102]

[100] *Kastelitz* in *Knyrim*[3] 106.
[101] See Recital 50 GDPR.

6.3. Rights of data subjects

The GDPR noticeably strengthens the rights of data subjects, i.e. those whose personal data is processed. The GDPR contains extensive information requirements for data collection, rights of access, rights of correction, deletion, limitation of processing and data portability, right of opposition and the right not to be subject to an automated individual decision. The claim is usually directed against the controller. The controller is obliged vis-a-vis data subjects to facilitate the exercise of their rights in accordance with Art. 12 (2) GDPR. The controller must, at the request of the data subject, pursuant to Art. 15 to 22 leg. cit., respond within a month. Although there are possibilities of extending the deadline, the reasons for this must also be communicated in the one-month period, so that in each case a quick response is required. If the company fails to comply with an application by the data subject, it faces a fine. The person responsible in the company must therefore implement processes that guarantee a timely and correct processing of the requests of the data subjects.

6.3.1. Art. 12 to 16 GDPR – The right to information

Art. 12 GDPR - Transparent information, communication and modalities for the exercise of the rights of data subjects

According to the principle of transparency at the start of processing there is already an obligation to provide comprehensive information to the data subject. Under Art. 12 GDPR, the controller must take appropriate measures to provide the data subject with all the data processing information in a clear, transparent, comprehensible and easily accessible form in clear and simple language. The information may be transmitted in writing or in another form, in particular also electronically; exceptionally it may also be transmitted orally provided that the data subject requested it and the identity of the data subject has been proven.

If an application (for example, for information) from a data subject reaches the controller, the controller can either take action and undertake measures, e.g. according to Art. 12 (3) GDPR provide information or waive provision. If the controller does not, however, take action, pursuant to Art. 12 (4) GDPR in addition to informing the data subject of this it must inform the data subject about the possibility of lodging a complaint with a supervisory authority or lodging an appeal to the court. If the controller takes action, pursuant to Art. 12 (3) GDPR, it must in principle respond promptly to the request of the data subject, but in any event within one month of receipt of the request. This period may be extended for a further two months, if

[102] *WKO OÖ*, EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung, wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html (Stand 29. 5. 2018).

necessary, taking into account the complexity and the number of applications. However, pursuant to Art. 12 (3) GDPR, the data subject must then be informed within one month of the extension of the time limit, stating the reasons for the delay. The information must be provided free of charge. In the case of manifestly unfounded or, in particular in the case of frequent repetition or excessive requests by a data subject, an appropriate remuneration or a refusal to act on the application may be claimed ; however, pursuant to Art. 12 (5) GDPR the controller has an obligation to provide proof in this regard.

Art. 13 GDPR – Duty to provide information when collecting data from the data subject

Personal data may be collected directly from the data subject pursuant to Art. 13 GDPR or from a third person pursuant to Art. 14 GDPR. Data collection from the data subject is to be assumed if the data subject had knowledge of the collection of their personal data or participated in the survey themselves.[103] If the survey takes place with the data subject themselves, pursuant to Art. 13 (1) GDPR, the controller must at the time of data collection inform the data subject of the processing in full and must provide the following information:

- Name and contact details of the controller and, if applicable, of its representative;
- Contact details of the data protection officer;
- Purposes of processing and legal basis;
- The legitimate interest of the person responsible, provided that the processing is based on Art. 6 (1) (f) GDPR;
- Where appropriate, recipients or categories of recipients;
- The intention to transfer the data to a third country/international organisation and the presence or absence of an adequacy decision by the Commission.

The following information must be made available to the data subject:

- Duration of data storage;
- Existence of a right of information, correction, deletion, limitation of processing, right to objection and right to data transferability,
- Right to revoke consent if processing occurs in accordance with (6) (1) or Art. 9 (2) (a) GDPR;
- The existence of a right to lodge a complaint with a supervisory authority;

[103] *Feiler/Forgó*, EU-DSGVO. EU-Datenschutz-Grundverordnung : Kurzkommentar (2017) Art. 13, 1.

- Information as to whether the provision of the personal data is required by law or is required for the conclusion of a contract and what the potential consequences of non-provision would be;
- The existence of automated decision making including profiling pursuant to Art. 22 (1) and (4).

If the controller intends to process the personal data for a purpose other than that for which the personal data was collected, this requires prior notification of the data subject. Regarding this other purpose and all other relevant information, pursuant to Art. 13 (2) GDPR it is necessary to examine whether such a change of purpose is permissible within the framework of Art. 6 (4) GDPR.[104]

By way of exception, pursuant to Art. 13 (4)GDPR, there is no obligation to provide information, as long as the data subject already has the necessary information.

This would mean that energy suppliers must already provide their customers the purpose of data processing when signing the contract. If the purpose changes or the data is also used for other processes, it must be examined whether this constitutes "further processing".[105]

Art. 14 GDPR – Duty to provide information if the data is not collected from the data subject

If the data is not collected from the data subject, the information requirements are very congruent with those in accordance with Art. 13 (1) and (2) GDPR . There are deviations, however, as follows:

- Notification of the categories of personal data being processed (such as customer data, employee data).
- Communication of the data source and whether it is publicly accessible.
- In addition, there is no need to be informed about the obligation to provide personal data or the need to fulfil the contract. Accordingly, there is no need to be informed of whether the information is voluntary or mandatory.[106]

Furthermore, in contrast to Art. 13 GDPR, more detailed regulations exist regarding the time the information is provided in accordance with Art. Art. (3) GDPR and the facts according to which the obligation to inform is waived pursuant to Art. 14 (5) GDPR.[107]

[104] *Fellner,* VbR 2018/47, 86f.
[105] See above, point 6..2.3."
[106] See *Feiler/Forgó*, EU-DSGVO Art. 14, 1f.
[107] *Fellner,* VbR 2018/47, 86ff.

In principle, the responsible company should be able to ensure that this data protection information complies with the above-mentioned requirements and, in particular, that proof of the communication of the information can be provided.

Art. 20 (1) (f) of the envisaged recast of the EltRL reflects Art. 14 of the GDPR. The information to be provided by the data protection officer is given when personal data is collected from the data subject. In particular, appropriate information on energy consumption and collection and processing of personal data must be provided at the time of installation of the smart meter. As regards the minimum information contained in the notice, the provision expressly refers to the applicable Union data protection legislation.

Article 20 (1) (e) of the new EltRL grants the customer the right to access their electricity input and output metering data, while Art. 23 (4) leg cit requires that this access should be free to end customers. Art. 20 describes the minimum principles to be observed when implementing smart metering systems. Data protection measures that enable the provision of information and the availability of measurement data therefore include a set of minimum functionalities that must be integrated into all smart metering systems. This is to be considered as an indication of the principle of data protection pursuant to the GDPR.

However, the right of access to the consumer's data is also guaranteed in a non-discriminatory manner and at the same time to all eligible third parties named in the new EltRL in order for the system to function properly. The access of entitled parties has its legal basis in Art. 23 (2) leg cit, which requires those responsible for data management to provide each party with access to the data of the end user, subject to its express consent, irrespective of the data management model chosen in each Member State. The access to the data of the consumers by the entitled parties is pursuant to Art. 23 (4) leg cit not necessarily free of charge. However, Art. 23 (4) leg cit requires Member States to set the appropriate access costs to ensure that regulated companies providing data services do not benefit from this process.

Art. 15 GDPR – Right to information

According to Article 15, a data subject has the right to know whether and to what extent personal data concerning them is processed by the controller. The right to information of the data subject about personal data stored with the controller is the central right, in order to claim further rights, e.g. the right to correction, deletion etc., if applicable. The data subject

may ask the controller for a confirmation as to whether personal data concerning the data subject is processed there. If this is the case, the data subject has the right to information on this personal data regarding:

- The processing purpose;
- The categories of personal data being processed;
- Recipients or categories of recipients to whom the personal data is disclosed, in particular third countries;
- If applicable, the planned storage duration, otherwise the criteria for determining this duration;
- Information on the rights to correction, deletion, restriction of processing and a right to object to processing;
- The right to lodge a complaint with the supervisory authority;
- Origin of the data, insofar as no survey has taken place with the data subject themselves;
- Where applicable, information about the existence of automated decision-making including profiling.[108]

If personal data is transferred to third countries/international organisations, data subjects have the right to be informed about the appropriate guarantees under Art. 46.

Depending on the circumstances, the possible form of provision of information may be in writing, electronically or orally, if possible in the form of a copy of the personal data pursuant to Art. 15 (3) GDPR. The controller must ensure that the information is provided only to the data subject or to a person authorised by the data subject, and that the rights and freedoms of other persons are not impaired.[109] Recital 63 refers to remote access of the data subject to their own data via a secure system as a data-protection-appropriate option.

Art. 16 GDPR – Right to correction

The data subject has the right to demand that the controller correct the personal data concerning the data subject if such data is incorrect. The right to correction must be met in the future without undue delay. Previously eight weeks were permitted for this. In consideration of the purposes of the processing, the data subject has the right to request the completion of incomplete personal data including by means of a supplementary statement.[110]

[108] *Wagner*, Die Datenschutz-Grundverordnung: die Betroffenenrechte (Teil IV), Dako 2015/59, 112 (112).
[109] *Fellner,* VbR 2018/47, 87f.
[110] *Feiler/Forgó*, EU-DSGVO Art. 16, 1f.

6.3.2. Art. 17 GDPR – Right to deletion, right to be forgotten

If a person no longer wishes their data to be processed and there is no legitimate reason to retain it, the personal data must be deleted by the processor. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press.

The data subject has the right to demand that the controller delete the data immediately if the following conditions are met pursuant to Art. 17 (1):

- The data is no longer necessary for the purposes for which it was collected or otherwise processed;
- The data subject revokes their consent in accordance with Art. 6 (1) (a) or Art. 9 (2) (a), and there is no other legal basis for the processing;
- The data subject objects to the processing and there are no prevailing legitimate grounds for further processing;
- The personal data was processed unlawfully,
- The deletion of personal data is required by a more specific law, i.e. to fulfil a legal obligation under Union or national law to which the data controller is subject;
- The personal data was collected from a child in connection with offered information society services.

This is about the idea of a “digital eraser”, which does not apply only to the online area. If the controller has made the personal data publicly available and is obliged to delete it under Art. 17 (1), under Article 17 (2) the controller must take appropriate measures, taking into account the available technologies and the implementation costs, to inform data controllers who process the personal data that a data subject has requested that they delete all links to such personal data or copies or replications of such personal data. Accordingly, a legitimate request for deletion by a data subject or the obligation to delete on the part of a controller entails the obligation to inform other controllers who are processing the data to be deleted about the request by the data subject regarding the deletion of links, copies or replications. It can be assumed that failure to do so, given the wording of the standard and the ongoing technical development, cannot be justified by a simple reference of the controller to an undue burden. The provision is, however, unclear about the specifics. According to the wording, the data subject must also require that their data be erased by other controllers. [111]

[111] Näher dazu *Feiler/Forgó*, EU-DSGVO Art. 18, 8.

Exceptions to this are contained in Art. 17 (3), which provides that the controller does not have to delete the data if further storage of the personal data is necessary for one of the following reasons:

- Exercise of the right to freedom of expression and information;
- Fulfilment of a legal obligation (e.g. statutory retention requirements) which requires processing under Union or Member State law or for the purpose of a public interest mission or in the exercise of official authority delegated to the controller;
- Reasons of public interest in the field of public health;
- Archival purposes of public interest, scientific or historical research purposes or statistical purposes;
- Assertion, exercise or defence of legal claims.

If any of the above reasons applies, a claim to deletion would already be terminated on the basis of the existence of a legal basis. And the processing would accordingly not be unlawful.[112]

6.3.3. Art. 18 GDPR – Right to restriction of processing

According to the Recitals[113], "restriction of processing" refers to methods of restricting the processing of personal data, e.g. that selected personal data is temporarily transferred to another processing system, that it is blocked for users or that published data is temporarily removed from a web page. The data subject has the right to require the controller to limit this processing if the following conditions are met:

- The accuracy of the personal data is disputed by the data subject for a period of time allowing the controller to verify the accuracy of the data;
- The processing is unlawful and the data subject declines to delete the data and instead requests a restriction of the processing;
- The controller no longer needs the personal data for the purposes of processing, but the data subject requires the personal data to assert, exercise or defend legal claims;
- The data subject has lodged an objection processing based on the legitimate interests of the controller, and it is not yet clear whether the legitimate reasons of the controller prevail over those of the data subject.

If the processing has been restricted at the request of the data subject, such personal data

[112] *Feiler/Forgó*, EU-DSGVO Art. 18, 9.
[113] See Recital 67 GDPR.

may only be used with the consent of the data subject or for the purpose of asserting, exercising or defending legal claims or protecting the rights of a natural or legal person or for important reasons of public interest of the Union or of a Member State. In addition, the controller must inform the data subject before the restriction is lifted[114].

6.3.4. Art. 21 GDPR – Right to objection

Data subjects have the right to object to processing unless there are compelling reasons for the processing. The GDPR also ensures the right of individuals to oppose direct marketing. If a person exercises this right, this means that both the transmission of direct marketing material and the processing of personal data for such marketing should be stopped.

The data subject may object to processing by the controller at any time if processing has been carried out on the basis of Art. 6 (1) (e) or (f) (assignment in the public interest or in the exercise of official authority, or for preservation of the legitimate interests of the controller). This also applies to profiling based on this. Continued processing by the controller is not permitted unless the controller can:

- Establish compelling legitimate grounds for processing that outweigh the interests, rights and freedoms of the data subject, or
- The processing serves the assertion, exercise or defence of legal claims.

No balance of interests takes place for direct marketing. An objection leads to the immediate cessation of the processing. In the event of processing for scientific or historical research purposes or for statistical purposes, the objection also leads to a cessation of processing unless the processing is necessary to fulfill a task of public interest (Art. 21 (6) GDPR).

The data subject must expressly be informed of their right to objection at the latest at the time of the first communication and in a form that is understandable and separate from other information.

6.3.5. Art. 22 GDPR – Profiling and automated decision-making

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which has a legal effect on them or similarly significantly affects them. In particular, the data subject has the right to require intervention on the part of the controller, to explain their own position and also to challenge the decision. The right not to be subjected to a decision based solely on automated processing does not apply if the decision:

[114] See Art. 18 (3) GDPR

- Is required for the conclusion or performance of a contract between the data subject and the controller;
- Is permitted by Union or Member State legislation to which the controller is subject, and where such legislation contains appropriate measures to safeguard the rights, freedoms and legitimate interests of the data subject; or
- The decision-making occurs with the express consent of the data subject.

7. Data protection impact assessment and prior consultation

7.1. Art. 35 GDPR Data protection impact assessment

As gathering detailed energy consumption data from smart grids and smart metering can create new risks for data breaches, data loss or data misuse at the household level, data protection in the smart grid area is an important issue, as already explained.[115] Another aspect that has now been enshrined in the GDPR by European legislation is the data protection impact assessment.

The data protection impact assessment is mandatory for organisations or institutions that initiate or already manage smart grid developments and make changes to existing smart grid architectures. By conducting a data protection impact assessment, organisations can take appropriate action to mitigate the identified risks, thereby minimising the potential impact of the risks on the individuals involved and reducing the risk of compliance violations or legal and operational risks. In addition, systems that have carried out a data protection impact assessment can have a significant competitive advantage because they have been analysed for privacy risks, which increases confidence in these systems.[116]
The data protection impact assessment is an evaluation and decision-making tool designed to help companies decide and plan the associated investments. It can reduce the risks of personal injury through misuse of personal information and can also be useful in developing more efficient and effective processes for the processing of personal data.[117]

The data protection impact assessment is a tool for describing the planned processing operations carried out by an organisation during its activities in order to assess the source, nature, specificity and severity of the risks of these measures for the rights and freedoms of data subjects. The results of the assessment help to identify the appropriate mitigating

[115] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018).

[116] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018).

[117] *Holzleitner/Reichl*, Legal problems for the protection of Smart Grids from Cyber Threats, European Energy Journal, 53 (60f).

measures and to demonstrate that the processing of personal data complies with data protection requirements.

7.1.1. Definition

The implementation of a data protection impact assessment (DPIA) is set out in Art. 35 of the GDPR and in Directive 2016/680[118].

Regarding the definition of a DPIA, it is possible to use the definition contained in the Guidelines of the Art. 29 Data Protection Impact Assessment Working Party (DPIA) that "a DPIA is a process by which the processing is described, its necessity and proportionality assessed and the risks assessed for the rights and freedoms of individuals resulting from the processing of personal data, which are to be better controlled through risk assessment and countermeasures". The DPIA is the key to accountability as it helps the controller not only in developing appropriate policies but also in complying with the requirements of the GDPR by providing evidence that appropriate action has been taken to comply with the Regulation.

Under GDPR, failure to comply with DPIA requirements may lead to fines imposed by the competent authority. Failure to implement a DPIA when processing or failing to properly conduct a DPIA, or failing to consult the data protection authority, although required, may result in a fine of up to EUR 10 million or, for a company, up to 2% of the annual total worldwide sales of the past fiscal year depending on which of the penalties would be higher.

The supervisory authority[119] compiles and publish a list of processing operations that require a data protection impact assessment, and the supervisory authority can also compile and publish a list of processing operations that do not require a data protection impact assessment.

There is also the possibility of the promotion of data protection certification programmes by the Member States. It aims to support the efficient implementation of the data protection impact assessment, especially for inexperienced and small-market actors. When performed by independent service providers, these systems can increase transparency and support the trust of end-customers.[120]

[118] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, and for free movement of such data, as well as the repeal of Council Framework Decision 2008/977/JI of the Council.

[119] See Art. 4 (21) GDPR, a "supervisory authority" is an independent body established by the State.

[120] *Expert Group 2*, Essential Regulatory Requirements an d Recommendations for Data Handling, Data Safety, and Consumer Protection,

7.1.2. When is a DPIA required?

The GDPR does not require that a DPIA be performed for all data processing that could pose risks to the rights and freedoms of individuals. Pursuant to Art. 35 (1) GDPR, the implementation of a DPIA is mandatory only if processing "probably represents a high risk to the rights and freedoms of natural persons". It is especially relevant when new data processing technology is introduced.

In cases where it is unclear whether a DPIA is required, the Art. 29 Working Party on Data Protection recommends that a DPIA be implemented anyway, as a DPIA is a useful tool to help data controllers comply with data protection law.[121]

Article 35 (3) contains a non-exhaustive list of cases where the processing "probably leads to high risks":

- Conducting a systematic and comprehensive assessment of personal aspects of natural persons based on automated processing - including profiling - which in turn will serve as the basis for decisions having legal effects on the natural person or similarly significantly affect the natural person;
- Processing of special categories of data pursuant to Art. 9 (1) or personal data relating to criminal convictions and offences in accordance with Art. 10 on a large scale;
- Systematic surveillance of a publicly accessible area on a large scale.

Recital 91 further points out that DPIAs must be carried out:

- In the event of large processing operations, which are aimed at the processing of substantial amounts of data and which could affect a large number of persons; or
- In accordance with the requirements of the supervisory authorities, which publish lists of processing operations falling under the requirement referred to in Art. 35 (1) - for example, when data processing prevents the data subjects from exercising a right or using a service or contract, or because it is systematically carried out on a large scale.

In its first recommendation for the introduction of smart measuring systems[122] published in 2012, the Commission invited the Member States to adopt and apply a template for the

ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1.pdf (Stand 2011)ff.

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

[122] Empfehlung der Kommission vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme, 2012/148/EU.

DPIA. This was subsequently developed by the Commission and submitted to the Art. 29 Working Party for its opinion. In 2013, the Commission submitted the first version of the DPIA template to the Art. 29 Working Party[123] created by a special expert group within the Smart Grid Task Force. In its opinion, the Art 29 Working Party welcomed the objectives set out in the proposal, but raised concerns in several areas and invited the Commission to revise them. A new version of the proposal was subsequently submitted to the Art. 29 Working Party. The final opinion of the Art. 29 Working Party of December 2013 recognised the improvements over the previous version and recommended that a test case be organised with some real cases. After taking into account these last comments from the Art. 29 Working Party, the Commission has published a recommendation to promote the adoption of the template.[124]

Although the recommendation of the Commission and the opinion of the Art. 29 Working Party were adopted before the formal adoption of the GDPR, they are fully in line with it. However, according to the new EltRL, there is no obligation to ensure that a DPIA is carried out, as a margin of discretion has been established when carrying out a DPIA for a smart meter. On the contrary, the GDPR makes the DPIA compulsory under certain conditions and calls on the supervisory authorities to impose fines if a compulsory DPIA is not carried out. According to the GDPR, a DPIA is only required if the processing "probably represents a high risk to the rights and freedoms of natural persons". In order to ensure a consistent interpretation of the circumstances in which a DPIA is compulsory, the Guidelines of the Art.29 Working Party[125], which were adopted in April 2017 and further revised in October 201, clarified this notion and set criteria for the development of a common EU list of processing operations for which a DPIA is compulsory. Although the European Commission

[123] *Expert Group 2*, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 1. 6. 2018).

[124] *Papakonstantinou/Kloza*, Legal Protection of Personal Data in Smart Grid and Smart Metering Systems from the European Perspective in *Goel/Hong/Papakonstantinou/Kloza*, Smart grid security (2015).

[125] *Article 29 Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

already has published a template for a DPIA for smart grids and smart metering systems[126], it does not specify clearly which companies need to conduct a DPIA.

The more criteria the processing meets, the more likely it is that it will present a high level of risk to the data subjects and therefore require a DPIA. Of the nine criteria named in the 2017 guidelines[127], at least three of these criteria seem to apply to the operation of smart meters. In particular, the rating or scoring criterion, including profiling and forecasting, is fully applicable to smart meters because the measurement data helps utilities to create behavioural or marketing profiles based on consumers' energy consumption. Data that is processed on a large scale may also be relevant in the context of smart meters. Smart meters collect consumption data at short, regular intervals and ensure timely delivery to data controllers or data aggregators that aggregate and manage huge amounts of data from consumers in a particular geographic area. This makes the efficient maintenance of the network possible, and energy suppliers can adjust their energy production accordingly. The criterion of innovative use/application of new technological or organisational solutions is undoubtedly also important for the use of smart measuring systems. Because these are novel forms of data collection and use with unknown, significant effects on a person's everyday life, a DPIA can help reduce the risks.

In addition, with a new technology product, a hardware or software application, which may be used by different data controllers and for different processing operations, may also trigger a need for a data impact assessment.

Although the controller remains obliged to implement its own DPIA for the specific implementation of the new product, a previously performed DPIA may be communicated to the subsequent customer. Regarding smart meters, this applies to the relationship between manufacturers of smart meters and distribution system operators or utilities. Each product supplier or processor should provide useful information without revealing any compromising secrets or information that could lead to security risks by exposing vulnerabilities.

7.1.3. DPIA process

The DPIA should be done "before processing". This is consistent with data protection through technology design and privacy-friendly preferences pursuant to Art. 25 GDPR. If a series of

[126] See Empfehlung der Kommission vom 10. Oktober 2014 über das Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme, 2014/724/EU.

[127] *Article 29 Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 9ff.

similar processing instances involves similar high risks, performing a single DPIA is sufficient to handle all of these processing instances.

DPIAs must contain the following minimum information[128]:

- A systematic description of the processing and purposes of the processing.
    - Where appropriate, the legitimate interest of the controller should be included;
- An assessment of the necessity and proportionality of the processing operations in relation to the application;
- An assessment of the risks to the rights and freedoms of data subjects,
    - Expectations of the data subject should also be included.
    - Assessment of the risk based on the likelihood and impact
- Measures to eliminate the risks,[129]
    - including security measures and mechanisms (e.g. pseudonymisation, anonymisation, encryption, local storage, access restriction, retention restrictions).
    - Compliance with the recognised rules of conduct must be taken into account.

The controller is responsible for performing the DPIA. The DPIA can be performed by someone else inside or outside the organisation, but the controller will ultimately be responsible for the task.

The controller must also seek the advice of the data protection officer if one has been appointed. The recommendation as well as the subsequent decisions must be documented in the framework of the DPIA. The data protection officer should also monitor the performance of the DPA.

If all or part of the processing is carried out by a commissioned processor, that processor must assist the controller in carrying out the DPIA and provide the necessary information.

[128] See Art. 35 (7) GDPR.
[129] See Art. 35 (3) GDPR.

8. Art. 20 GDPR – Right to data portability

Art. 20 GDPR introduces the new right to data portability. Under this provision, data subjects have the right to receive the personal data relating to them, which they have made available to a controller, in a structured, common, machine-readable and interoperable format and to transmit this data to another controller without hindrance. This right, subject to certain conditions, encourages user choice and control and consumer empowerment. The right to data portability should facilitate the switchover to various providers including energy providers.

As can be seen in Recital 68, the data subject's right to data portability is intended to give the data subject better control over their data by giving them access to the data themselves. In order to assert the right pursuant to Art. 20 (1) GDPR, three conditions must be met:

- Processing is based on consent or contract;
- The controller uses automated procedures for processing; and
- The data subject has provided the data themselves.

Data which the data subject has actively transmitted to the controller is of course self-provided. However, according to the interpretation of the Art. 29 Working Party, this includes data collected through the use of the controller's service, such as smart meter raw data, log files, location data at mobile operators etc.[130] Accordingly, the following data are considered to have been provided:

- Data that a data subject has actively and knowingly provided to or communicated to the controller (e.g. disclosure in the context of a contract declaration or information provided by the data subject in forms such as name, address, date of birth);
- Recorded data generated by the data subject using a service or device of the controller (including smart meter raw data)[131];

According to *Hübelbauer*, data collected by the controller from third parties based on an authorisation given by the data subject is also included. The authorisation constitutes

[130] *Article 29 Working Party*, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (abgefragt am 1. 6. 2018), 9ff.

[131] See *Hübelbauer*, DSGVO: Das Recht auf DSGVO: Das Recht auf Datenübertragbarkeit (Teil XIII), Dako 2017/64, 106 f.

consent to the collection of data and therefore the information path is shortened. In any case, explicit consent and thus an active and knowledgeable action of the data subject is required.

If the processing is based on another justification, e.g. the fulfilment of a legal obligation or the overriding legitimate interest of the controller or a third party, the right to data portability does not exist.[132] This may be relevant for the period after termination of a contract: For the storage of personal data for the purpose of fulfilling the requirements of storage and documentation, as a rule no consent is present; the respective statutory provision, such as § 132 BAO[133], is appealed to instead - In this case the right to data portability would not apply.[134]

The right to data portability does not apply to processing in the public interest or under public authority. These concern, however, independent legal bases pursuant to Art. 6 GDPR, in which the conditions requiring consent or a contract probably are met in very few cases.[135]

Pursuant to Art. 20 (1) and (2) GDPR, the data subject has the right to data portability and therefore the following claims to:

- Provision of "the data subject's" data in a structured, common and machine-readable format;[136]
- Retransmission without hindrance ;[137]
- Direct transmission to other recipients (as far as technically feasible) by the controller.

According to Art. 20 (1) GDPR, the transmission must occur in a "structured", "common" and "machine-readable"[138] format - fulfilling these three requirements should lead to interoperable systems. However, according to Recital 69, there is no obligation on the controller to adopt or

[132] See Art. 20 (1) and (3) and Recital 68 GDPR.

[133] Federal law on general provisions and the procedure for the taxes managed by the tax authorities of the federal government, the federal states and the municipalities (Federal Tax Code - BAO), BGBL 194/1961 (as amended) BGBl. I 32/2018.

[134] See *Hübelbauer,* Dako 2017/64.

[135] See *Knyrim* (Hrsg), Datenschutzrecht[3] (2015), 165ff.

[136] For more information, see *Article 29 Working Party*, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (abgefragt am 1. 6. 2018) 15 ff.

[137] Examples of disabilities *Article 29 Working Party*, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (abgefragt am 1. 6. 2018), 15.

[138] See idZ Art 2 Z 6 RL 2003/98/EC of the EP and of the Council of 17/11/2003 on the re-use of public sector information, as amended by RL 2013/37/EU of the EP and of the Council of 26/6/2013, where "machine-readable format" is defined as "a file format that is structured so that software applications can easily identify, recognise, and extract specific data, including individual factual representations and their internal structure."

maintain technically compatible data systems. However, the Art .29 Working Party recommends that interoperable standards and formats be established within an industry or sector such as those of energy suppliers.[139]

Interoperable systems are those that are designed so that the reusability of the data and the processing of the data is fully possible. The GDPR is formulated in a technology-neutral way; therefore all formats could be considered adequate, which are structured, common and machine-readable. Expensive licenses are not considered an appropriate approach by the Art. 29 Working Party. Those responsible should use the data to transfer as much metadata as possible at the best granularity level to preserve the significance of the information being exchanged. Metadata should be large enough to allow the use and reuse of the data without disclosing trade secrets. Possible file formats include XML, JSON and CSV.[140]

If a request for data portability is made it must be implemented within for weeks pursuant to Art. 12 (3) GDPR. If there is special complexity[141] or if there are a large number of requests, the deadline can be extended by a further 2 months. If the controller assumes that Art. 20 GDPR is not applicable, it must notify the controller within one month.

The billing of costs in connection with the transfer of data should be inadmissible since the effort for the implementation of required IT systems should not be passed on to data subjects.

According to Art. 20 (3) GDPR, the right to data portability does not affect the right to deletion. Accordingly, if the end user changes their energy supplier and requires transfer of data to the new supplier, the old supplier does not have to delete the data subject's data and is still entitled to keep it until the end of the retention period.

Pursuant to Art. 20 (4) GDPR, the right to data portability must not affect the rights and freedoms of third parties. This predominantly concerns the personal rights of other natural persons. According to the Art. 29 Working Party, the transfer of data, for example, from private webmail or bank accounts kept by the data subject for personal or family purposes, is unobjectionable in this regard. This can be seen differently if the "new" person controller

[139] *Article 29 Working Party*, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (abgefragt am 1. 6. 2018),18.

[140] *Article 29 Working Party*, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (abgefragt am 1. 6. 2018), 18f.

[141] For example, with very large amounts of data, complicated data structures or use of different IT systems.

wants to process the data for its own purposes. The (new) controller, who receives data and to whom the data can be transmitted on request of the user, may not use the transmitted data of third parties for its own purposes. This is only permitted for the purpose for which the processing took place prior to the data transfer in accordance with Art. 20 GDPR. In these cases, the Art. 29 Working Party recommends the implementation of a best practice in order to allow the data subject to select the data of other data subjects. This should reduce the risks for third parties whose personal data could possibly be transferred together with the other personal data. In addition, consent mechanisms for other data subjects can be introduced. [142]

Art. 20 (4) GDPR can also be interpreted to mean that proprietary interests, such as those of the controller, are also protected. The Art. 29 Working Party mentions, for example, intellectual property rights and confidential business information.[143]

The planned new version of the EltRL welcomes this focus on the industry and sets out the minimum characteristics that the format for the transmission of measurement data should have. Article 20 (1) (e) of the new EltRL stipulates that metering data for the supply and withdrawal of electricity must be provided via a local standardised interface and/or remote access in an easily understandable format so that customers can compare offers under the same conditions. The main goal of data portability pursuant to Art. 20 GDPR appears to be price comparability in order to facilitate change of service and to increase competition between services. This provision corresponds precisely to Art. 24 of that Directive, which requires Member States to develop a common data format and a transparent procedure for eligible parties to access consumer data. Here too the focus is on competition, because the data format is intended to ensure that the energy providers operating on the retail market receive simultaneous and non-discriminatory access to the end customer data. However, the new EltRL does not contain minimum specifications for the access data format for authorized parties. This will be decided by the Member States and then by the Commission, which is explicitly invited to establish a common European data format replacing all data formats used

[142] *Article 29 Working Party*, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (abgefragt am 1. 6. 2018), 11f.

[143] *Haidinger*, Die Rechte auf Löschung, Berichtigung, Einschränkung und Datenübertragbarkeit nach der DSGVO (Teil XI), Dako 2017/34, 56.

at the national level. However, in Austria, a uniform European data format has clearly been rejected because of difficulty in implementation.[144]

9. Conclusions

The "Winter Package" also already addresses the innovations in the energy sector. According to the current state of the Internal Market in Electricity Directive, electricity customers should be able to access their consumption data free of charge in the future. The customers must be able to decide for themselves to which other companies - e.g. electricity providers, network operators and aggregators - they want to pass on their data or have it passed on[145].

The company managing the electricity consumption data must grant other companies non-discriminatory access to the consumption data with the consent of the electricity consumers. [146]

In addition, the Commission will adopt a transposition act establishing a common data format and procedure for the dissemination of electricity consumption data.[147]

Member States must set prices for access by other companies[148].

If a consumer changes their place of residence, they have a claim against the network operator and the energy supplier to take their electricity consumption data with them from the old residence to their new residence. However, the new electricity supplier is not required to record the data of the old residence in its "customer portal".

Smart metering systems are becoming one of the most important tools for promoting participatory processes and decentralisation, which are at the heart of the energy revolution and the development of new energy services. Since the Third Energy Package has made the introduction compulsory and the "Winter Package" is the central instrument for more efficient energy consumption, an even greater use of smart meters in the near future is to be expected. The potential privacy risks associated with the introduction of smart meters must be given top priority. So it is essential that consumers have access to trusted mechanisms to

[144] See *Österreichs Energie*, Stellungnahme zum Vorschlag der Europäischen Kommission Elektrizitätsbinnenmarkt-Richtlinie (COM(2016) 864 final), oesterreichsenergie.at/files/Download%20Stellungnahmen/Stellungnahmen%202017/ST_EU%20Elektrizit%C3%A4tsbinnenmarktRL.pdf (abgefragt am 16. 6. 2018).

[145] See Art. 23 (1) in conjunction with Art. 24 (3) COM(2016) 864 final.

[146] See new Art. 34. COM(2016) 864 final.

[147] See Art. 24 (2) COM(2016) 864 final.

[148] See Art. 23 (4) COM(2016) 864 final.

manage their energy data. For example, consumers can add value to energy efficiency by monitoring their private environment and their behaviour habits.

A series of legislation has been adopted to reconcile energy policy objectives with data protection concerns. In recent years, the EU legislator has begun to pay particular attention to the protection of personal data with regard to the introduction of smart meters and, as a result, some important progress has been made, such as the development of the DPIA scheme.

Today, the development of privacy standards and safeguards, as well as the security of smart metering, is an important EU goal. Against the background of the GDPR, the planned revision of the EltRL proposes a specific data protection and security framework for smart meters. The aim is to introduce relevant GDPR provisions in the new version and to adapt them to the needs and characteristics of the introduction and functioning of smart meters. It follows that a new comprehensive legal framework will be set up to ensure a high level of protection of personal data in smart metering systems, which should increase the confidence of energy consumers and thus increase their participation in decentralisation.

10. Bibliography

Angerler et al, Datenschutz-Grundverordnung. Praxishandbuch (2016).

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

Article 29 Working Party, Leitlinien zum Recht auf Datenübertragbarkeit, ec.europa.eu/justice/data-protection/index_en.htm (1. 6. 2018).

Buschmann/Motyka, Energieeffizienz als Schlüssel zur Klima- und Ressourcenschonung? – am Beispiel des Smart Metering, wbl 2011, 11–17.

Dürager/Kotschy, Neuerungen zur Zustimmung (Einwilligung) nach der DS-GVO. Debattenbeitrag zur Datenschutz-Grundverordnung (21. 6. 2018).

Energie Burgenland, Online Customer Centre, kundencenter.energieburgenland.at/okc-energie/static.xhtml?id=1522&dswid=-8257 (21. 6. 2018).

Energie-Control Austria, Information about supplier change, e-control.at/industrie/strom/lieferantenwechsel/ (21. 6. 2018).

European Commission, Commission recommendation of 9 March 2012 on preparations for the introduction of smart metering systems, 2012/148/EU.

European Commission, Commission recommendation of 10 October 2014 on the model for data protection impact assessment on smart grids and smart metering systems, 2014/724/EU.

European Commission, Legal Opinion – Legal Aspects of European Energy Data. Output 2 of the "Study on the quality of electricity market data" commissioned by the European Commission, 1–25.

European Commission, Commission proposes new rules for consumer centred clean energy transition - Energy - European Commission, ec.europa.eu/energy/en/news/commission-proposes-new-rules-consumer-centred-clean-energy-transition (14. 6. 2018).

European Commission, Proposals on clean energy for all Europeans, ec.europa.eu/commission/priorities/energy-union-and-climate/proposals-clean-energy-all-europeans_en (14. 6. 2018).

European Commission, Data protection, ec.europa.eu/info/law/law-topic/data-protection_en (13. 6. 2018).

Expert Group 2, Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment. Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (1. 6. 2018).

Expert Group 2, Essential Regulatory Requirements an d Recommendations for Data Handling, Data Safety, and Consumer Protection. Recommendation to the European Commission, ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1.pdf (13. 6. 2018).

Feil, Rechtliches zu Apps und App-Entwicklung, anwalt.de/rechtstipps/rechtliches-zu-apps-und-app-entwicklung_057414.html (14. 6. 2018).

Feiler/Forgó, EU-DSGVO. EU-Datenschutz-Grundverordnung : Kurzkommentar (2017).

Fellner, Betroffenenrechte nach der DSGVO, VbR 2018/47, 84–89.

Fratini/Pizza, Data protection and smart meters: the GDPR and the 'winter package' of EU clean energy law, eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html (14. 6. 2018).

Goel/Hong/Papakonstantinou/Kloza, Smart grid security (2015).

Grabenwarter/Graf/Ritschl, Neuerungen im europäischen Datenschutzrecht (2017).

Haidinger, Die Rechte auf Löschung, Berichtigung, Einschränkung und Datenübertragbarkeit nach der DSGVO (Part XI), Dako 2017/34, 56–59.

Holzleitner/Reichl, Legal Problems for the Protection of Smart Grids from Cyber Threats, European Energy Journal, 53–61.

Hübelbauer, DSGVO: Das Recht auf DSGVO: Das Recht auf Datenübertragbarkeit (Part XIII), Dako 2017/64, 106–108.

2014 18th IEEE International Symposium on Power Line Communications and Its Applications (ISPLC). March 30, 2014 - April 2, 2014, Glasgow, Scotland (2014).

Jahnel, Datenschutzrecht. Jahrbuch 2014[1] (2014).

Jahnel, Datenschutzrecht. Jahrbuch 2016[1] (2016).

Jahnel, Datenschutzrecht. Jahrbuch 2017[1] (2017).

Kanzlei Dr. Bahr, IT-Recht für App-Entwickler: Rechte und Pflichten, zdnet.de/41553406/it-recht-fuer-app-entwickler-rechte-und-pflichten (13. 6. 2018).

Kastelitz, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 5-11 DSGVO), in *Knyrim* (Ed.), Datenschutzrecht. Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm[3] (2015) 99–136.

Knyrim (Hrsg), Datenschutzrecht. Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm[3] (2015).

Leissler, Apps & Datenschutz. Jetzt auch als APP, ipCompetence 2012 H 8, 46, 46–54.

Mengi/Waechter/Koch, 500 kHz G3-PLC access technology for the roll-outs in Germany, in 18th IEEE International Symposium on Power Line Communications and Its Applications (3/30/2014 - 4/2/2014) 179–183.

Ohishi/Hashimoto (Hrsg), IECON 2015 - Yokohama. 41st Annual Conference of the IEEE Industrial Electronics Society : November 9-12, 2015, Pacifico Yokohama, Yokohama, Japan (2015).

Austria's Energy , General information on change of supplier, oesterreichsenergie.at/lieferantenwechsel.html (21. 6. 2018).

Österreichs Energie, Opinion on the proposal of the European Commission for the Electricity Market Directive (COM (2016) 864 final), oesterreichsenergie.at/files/Download%20Stellungnahmen/Stellungnahmen%202017/ST_EU%20Electricity_International_RLRL.pdf (16. 6. 2018).

PwC Österreich, Study to analyze the cost-benefit of an Austria-wide introduction of Smart Metering, e-control.at/documents/20903/-/-/cf11cc28-2826-4bf8-95e1-59ba8c75dac3 (13. 6. 2018).

Renner, Smart Metering und Datenschutz in Österreich, In:, Datenschutz und Datensicherheit (DuD), 524–529.

Schrott, (Masters Thesis) Die Datenschutz-Grundverordnung: Das neue Datenschutzrecht und die Auswirkungen auf Energieversorgungsunternehmen (2017).

Schwenke, Die rechtlichen Rahmenbedingungen der App-Entwicklung, textintern 2012, 6–9.

Shiobara/Palensky/Nishi, Effective metering data aggregation for smart grid communication infrastructure, in *Ohishi/Hashimoto* (Hrsg), IECON 2015 - Yokohama. 41st Annual Conference of the IEEE Industrial Electronics Society : November 9-12, 2015, Pacifico Yokohama, Yokohama, Japan (2015) 2136–2141.

Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit. Rechtliche, technische und verbraucherbezogene Implikationen, stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/studie-datenportabilitaet.pdf (1. 6. 2018).

Unverzagt von Have, Neue Hinweise der Datenschutzbehörden zum Datenschutz im Mobile Bereich | Online-Marketingrecht, onlinemarketingrecht.de/2014/10/neue-hinweise-der-datenschutzbehorden-zum-datenschutz-im-mobile-bereich/ (13. 6. 2018).

Wagner, Die Datenschutz-Grundverordnung: die Betroffenenrechte (Part IV), Dako 2015/59, 112–115.

WKO OÖ, EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung, wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html (13. 6. 2018).

ZfK, Study: One third of all German companies fear EU data protection regulation, zfk.de/digitalisierung/it/artikel/studie-ein-drittel-aller-deutschen-unternehmen-fuerchten-eu-datenschutzgrundverordnung-2018-02-20/ (13. 6. 2018).