700416 SUCCESS

D3.15 V1.0

Guidelines and Blueprints for data privacy in Real Time Energy Services

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700416.

Project Name	SUCCESS
Contractual Delivery Date:	31.10.2018
Actual Delivery Date:	31.10.2018
Contributors:	VUB
Work package:	WP3
Security:	PU
Nature:	R
Version:	1.0
Total number of pages:	35

Abstract:

The purpose of this deliverable is to give a comprehensive view on privacy and data protection in the context of real time energy services. Accordingly, details are provided about the privacy-by-design solutions elaborated in the context of SUCCESS.

In addition, this deliverable goes beyond the specific context of SUCCESS project. With the aim of reaching a new era of personal data management within real time energy services, it extrapolates, from the particular context of SUCCESS, a series of general recommendations generally implementable. The good example of SUCCESS, in fact, can be usefully spent not only within the project boundaries, but also in the whole real time energy distribution sector.

Keyword list:

Privacy, Data Protection, Data Protection Impact Assessment, Privacy Impact Assessment

Executive Summary

The deliverable collects data protection recommendations, guidelines and best practices for the energy grid, and summarizes relevant technical solutions developed within the SUCCESS project, so that they can be exported and implemented outside the project when dealing with real time energy distribution.

In order to do so, this deliverable is based on three basic steps:

- Resuming the related *privacy principles* in the primary and secondary EU legislation (Section 2);
- Recalling the technical privacy-by-design solutions developed within SUCCESS project (Section 3);
- Extrapolating from these *ad hoc* solutions *privacy guidelines* and *best practices* for the energy sector (section 4).

Authors

Partner	Name	e-mail
Vrije Universiteit Brussel		
	Gianclaudio Malgieri	gianclaudio.malgieri@vub.ac.be
	Giorgia Bucaria	giorgia.bucaria@santannapisa.it
	Paul De Hert	paul.de.hert@uvt.nl

Table of Contents

1. Introduction

1.1 Scope of this deliverable

Smart meters are currently subject to vibrant public debates. Given the crucial role of the energy sector for the development of economy and society, the roll-out of smart technologies in energy distribution has been warmly welcomed by policy makers of several countries and, in the first place, by EU institutions. However, standing the overall positive effect that a massive deployment of smart grids would have on the general economy of the energy sector, doubts remain concerning the impact that the roll-out of these newly developed technologies may have on the rights and freedom of end-users.

Due to the fact that the functionality of smart grids strongly depends on the data collected by smart meters, the deployment of the newly developed smart grid technologies is strongly interrelated with privacy and data protection law. Not only the concerns of end-users, but also the necessity to comply with the data protection legal framework force us to analyse those technologies with the aim of investigating and facing the challenges that characterise smart grids from a privacy and security standpoint. The collection, retention, sharing, or reuse of data, that is necessary for the functioning of the smart grid, is an issue that has to be carefully considered under the lens of the risks it poses to the end-users' privacy. As the data produced by a smart grid are able to offer **sharp insights into consumers' energy use** (and consequently **into their end-users' private habits at home**), there is a great urge to respond to this problem by striking a careful balance between the necessity of detailed energy metering (so as to achieve an efficient energy distribution) and the security and protection of the data involved (so as to consent an high degree of privacy of customers). It is commonly said, in fact, that, in response to the risks that the massive deployment of smart grid technology is able to pose, the legal frameworks on privacy and data protection plays the role of external limits and safeguards.

Accordingly, this deliverable describes relevant and effective steps in order to translate Privacy and data protection principles into practical privacy-by-design solutions for a new era of data management within real time energy services.

1.1.1 Structure and chapter contents

Looking at the massive amount of pieces of legislation and official documents issued in this respect, it is clear that a work of **recognition and reorganisation of the material** concerning privacy and smart grids is needed. The multi-layer approach followed by EU institutions, in fact, albeit appropriate for the purpose of adapting quickly to the rapidly changing needs of this sector, has brought about confusion, fragmentation and thus uncertainty in the practical application of the data protection legal framework.

Accordingly, the purpose of this deliverable is to **recap and harmonise** the legal background with the aim of smoothening its practical application. Furthermore, it will be useful to focalise precisely what provisions play a major role in the context of smart grids and how the general principle of data protection law can be specified according to the specific features of smart grid environment.

With this aim in mind, this deliverable will be structured as follows:

- In section 2 (fundamental notions from the Data Protection framework) we will recap the basic principle of data protection law, as well as some simple definitions of its essential elements;
- In paragraph 3 (Privacy-by-design solution in SUCCESS) the main focus will be on the solutions that have been specifically orchestrated in the context of SUCCESS;
- In paragraph 4 (Lessons from the good example of SUCCESS) we will elaborate a list of guidelines and best practices useful for the whole energy sector (and especially in the case of real time energy services) when dealing with privacy-sensitive issues;
- The conclusion, instead, aims to sum up the results of SUCCESS project.

1.2 Relationship to the work of the project

As mentioned, this deliverable is fundamental to achieve the main goals of the SUCCESS project. In fact, without a careful assessment of the potential privacy infringements that come as inherent

risks of the massive roll-out of real time energy services, the rights and freedoms of the service recipients are in jeopardy. This would have a negative impact on the results of the SUCCESS project.

This deliverable has been produced within the activities of Work Package 3 as the natural development of the deliverables 3.1, 3.2 and 3.3, concerning the topic of privacy preserving information security architecture. However, while the purpose of the previous deliverables (3.1, 3.2, 3.3) was to elaborate adequate measures to ensure compliance within this specific project, on the contrary the deliverable at issue (3.15) is the result of a wider approach to the topic. In other words, regardless of the specific features of SUCCESS components and architecture, we tried to outline a general framework for the benefit of all the stakeholders dealing with personal data in the energy distribution sector. This purpose is strictly connected with the operations of the Work Package 4 and, more precisely, whit the deliverable 4.10, where we proposed an innovative approach for data privacy for energy services.

1.3 How to Read This Document

This deliverable can be considered as the final step towards the conclusion of the project. It should be, in fact, read as a stand-alone document. On the one hand, it sums up the results of the previous deliverables, with specific reference to the privacy-by-design solutions exposed there. On the other hand, it is an attempt to go further, not only by carrying out a more in-depth analysis of the topics already mentioned (e.g. the legal bases) but also reorganising them in a more accessible and user-friendly form. Finally, while the previous deliverables were focused on the specific context of SUCCESS, here It seemed necessary to widen the scope of the analysis to the whole energy distribution sector, so as to provide a comprehensive set of guidelines generally implementable.

2. Fundamental notions from the Data Protection Framework

2.1 The legal background

The data protection framework plays a fundamental role in assessing the lawfulness of smart grid technologies. Therefore, before proceeding to the analysis of the legal provisions specific to the smart grid context, it is necessary to provide a general oversight of data protection law. Accordingly, here we listed the legislation pieces representing the necessary background for the subsequent analysis:

- Art. 8 of the European Convention on Human Rights (right to private and family life);
- Art. 7 of the European Union Charter of Fundamental Rights (right to private and family life);
- Art. 8 of the European Union Charter of Fundamental Rights (right to protection of personal data);
- General Data Protection Regulation (Reg. EU 2016/679);
- E-privacy directive (Directive 2002/58/EC);
- NIS Directive (Directive EU 2016/1148) concerning measures for a high common level of security of network and information systems across the Union;
- Council Directive on European Critical Infrastructures (Directive 2008/114/EC).

2.1.1 Getting more specific

Obviously, the starting point to address the privacy issue in the use of smart grid technologies is the data protection framework (at the moment, the GDPR - Reg. EU 679/2016). However, the GDPR comes with a burgeoning number of official documents dealing with the issue of privacy in the context of real time energy distribution. This resulted in the creation of a complex multi-layer approach towards personal data protection aspects in the context of smart meters, which may result in difficulties to use it in practice[1].

Thus, the European Commission decided to launch the **"Smart Grids Task Force"** (in 2009), including, in the composition of one of the four groups formed on this basis, an experts group charged with providing **regulatory recommendations for privacy, data protection and cyber-security in smart grids and metering environments[2].** On the basis of the results of their work, the **European Commission issued** (in 2012) **a non – binding recommendation on the roll out of smart grid and smart metering systems[3]**.

The aspects addressed by the 2012 Recommendation are: 1) **personal data protection,** 2) cost-benefit analysis, and 3) **common minimum functional requirements of smart meters**.

Focusing the attention on the first aspect, it is clearly pointed out that «*the 1995 Data Protection Directive applies and clarifies its application to the nature and needs of smart grids*». Furthermore, it lists six "tools" that are deemed to be necessary for the purpose of achieving a fair level of compliance with the data protection regulatory framework: **1) Data protection by default and by design**; **2) Privacy certification, Privacy Enhancing Technologies (PETs)**, in particular **anonymisation** and **encryption**; **3) Best Available Techniques (BATs);** and **4) Data Protection Impact Assessment (DPIA).**

The 2012 Recommendation is not the sole document issued by the European commission: The action framework it provides in order to **tackle privacy and data-protection aspects in smart grids and smart metering environments** has been supplemented by several **opinions**, **guidelines** and **studies by relevant bodies** within or interacting with **the European**

---

[1] Dariusz Kloza, Niels van Dijk and Paul De Hert, 'Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies' [2015] Smart Grid Security: Innovative Solutions for a Modernized Grid, p.13.

[2] Cf. http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task- force

[3] European Commission, *Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems*, 2012/148/EU, OJ L 73, 13.03.2012, pp. 9-22 (*hereinafter*: the 2012 Recommendation).

Commission. For example, the Article 29 Working Party opinion WP183 on smart metering is a useful tool, able to provide the reader with further guidance on the processing of Smart Metering data and compliance with the Data Protection regulatory framework.

The necessity to take in due consideration privacy and data protection when talking about smart grid technology deployment is further confirmed by the **2012 Energy Efficiency Directive.** Under art. **9.2.b**: «Where, and to the extent that, Member States implement intelligent metering systems and roll out smart meters […] they **shall ensure** the **security** of the **smart meters** and **data communication**, and the **privacy of final customers**, in compliance with **relevant Union data protection and privacy legislation».**

The efforts of the Commission did not stop here and an *ad hoc template for the development of **Data Protection Impact Assessments** when **intelligent metering systems are deployed*** has been elaborated**.** The first phase of this process resulted in the adoption of another **recommendation** of the Commission **on the Data Protection Impact Assessment Template** for Smart Grid and Smart Metering Systems (hereafter the 2014 Recommendation)[4].

2.2 Basic notions from data protection law

Below is a list of requirements from data protection law **identified as important for any security countermeasure that the SUCCESS project will develop.** We believe, in fact, that no analysis can start without a clear definition of its object. Applying this common-sense principle to this context, we strongly recommend a general knowledge of **the basic elements** and **the general principles** that rule data protection law. As a consequence, we decided to provide the reader with a brief discussion about a number of concepts from the general data protection legal framework that emerged as relevant. Also the essential principles of data protection law will be examined.

2.2.1 The notion of Personal Data

First of all, a discussion about the notion of *personal data* is needed. Under art. 4(1) of the GDPR (Reg. EU 679/2016) what is considered to be a *personal data* is «any **information** relating to an **identified or identifiable natural person** ('data subject') ». In the same article we can find a definition of the concept of *identification*: «an identifiable natural person is one who can be identified, directly or indirectly through an *identifier*». It also provides a non-exhaustive list of the **identifiers** that, when in connection with an information, are thought to make it a *personal data*. This list specifically refers to «name, identification number, location data, and online identifier» but also general factors «specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person» are mentioned. Obviously, not all the identifiers have the same value in investigating the actual possibilities of identifying a subject. That is why recital 26 proposes **a risk-based approach** in order to assess the "personality" of data: «to determine whether a natural person is identifiable[5]» it is necessary to take into consideration «all the means reasonably likely to be used[6]» on the basis of «objective factors, such as the costs of and the amount of time required for identification» considering the «available technology[7]».

2.2.1.1 Legal persons' data

It is important to notice that, albeit the broadness of the notion of personal data, **the protection of data privacy applies <u>only in cases where final customers (or their data)</u> are involved**. This is confirmed by a number of provisions of the GDPR

[4] European Commission Recommendation (2014/724/EU) providing guidance to Member States on measures to be taken for the positive and wide ranging dissemination, recognition and use of the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems.

[5] Recital 26, Reg. EU 679/2016 (GDPR)

[6] *Ibid.*

[7] *Ibid.*

- A systematic reading of art. 4(1)[8] and art. 2, par. 1[9] of the GDPR (Reg. EU 679/2916) explicitly excludes the application of the data protection regulatory framework where there is no individuals' involvement: only data that *regards* natural persons (identified or identifiable individuals) are in the material scope of the regulation.
- This interpretation is further confirmed by art. 1(1) of GDPR (Reg. EU 679/2916). The article, in defining the "**subject-matter and objectives**" of the Regulation, clearly affirms that the Regulation «lays down rules relating to the protection of **natural persons** with regard to the processing of personal data» and that it is finalised to the protection of «fundamental rights and freedoms of **natural persons**».
- Moreover, recital 14 of the GDPR completes the scenario by restating that «the protection afforded by this Regulation should apply to *natural persons*, […], in relation to the processing of their personal data». It also adds a fundamental explanation: «This Regulation **does not cover the processing of personal data which concerns legal persons** *and in particular undertakings established as legal persons*, *including the name and the form of the legal person and the contact details of the legal person*».

For the protection of data concerning legal person and, more specifically, **for the protection of data and information that are relevant in the context of competition policies**, the EU legal framework offers a different legal tool: the **protection of trade secrets[10]** (Dir. EU 2016/943[11])[12]

Obviously, when information, albeit concerning primarily and directly a legal person, is potentially able to include data regarding a natural person (such as, for instance, personal data of legal persons' customers, members or partners), then the GDPR applies.

2.2.1.2 Special categories of data

Under art. 9 of the GDPR, the processing of data «revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation» is not allowed. This provision is justified by the fact that this type of information can easily lead to sensitive discrimination and to a form of limitation of the rights and freedom of the data-subject, as pointed out by recital 51[13] of the GDPR (Re. EU 679/2016). However, under specific circumstances the processing of such data is permitted. Those circumstances are listed in art. 9.2 from (a) to (j). Among these exceptions, we find also the case where the data-subject has given explicit consent to the processing of those personal data for one or more specified purposes[14].

---

[8] Art. 4 (1), Reg. EU 679/2016 (GDPR): «'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person»

[9] Art. 2, par. 1, Reg. EU 679/2016 (GDPR): «This Regulation applies to the processing of personal data […]»

[10] About the relationship between data privacy and trade secrets see Gianclaudio Malgieri, *Trade secrets v. Personal Data: A Possible Solution for Balancing Rights*, International Data Privacy Law, First published online: January 29, 2016.

[11] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance).

[12] Please notice that the protection of trade secrets cannot be considered within the scope of this deliverable, which is explicitly focussed on "data privacy compliance" of SUCCESS Solutions

[13] «Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms».

[14] This can be done except where Union or Member State law provide that the general prohibition may not be lifted by the data subject (art 9.2.a of GDPR).

2.2.2 The notion of anonymous data

The notion of anonymous data is fundamental in data protection law. The concept of anonymity, in fact, is necessary to properly define the material scope of the data protection framework as, if the data is anonymous, the GDPR does not apply. The notion of anonymity is not crystal clear. However, we can say that, if a data is considered personal when it regards directly or indirectly a natural person, by contrast the anonymous data is an information that cannot be connected to a natural person, so that the identification of the subject is impossible.

According to recital 26 of the GDPR, the concept of personality and anonymity of data are to be investigated according to a risk-based approach, able to catch all the shades of the matter of fact. In fact, «to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used[15]». This leads to the consequence that a data cannot be considered "anonymous" *per se*: the evaluation about the anonymity of data should take into account all the circumstance at stake, such as the identity of the person who has the data and the means in his or her disposal.

2.2.3 The notion of pseudonymised data

Data can be considered pseudonymised when the identifiers that provide the identification of the data subject are replaced with artificial identifiers (pseudonyms), such as unique number or alphanumeric codes. This process is strongly advised in order to reduce data protection concerns and data breaches. Furthermore, pseudonymisation is also a useful tool to increase processing efficiency.

The difference between pseudonymised and anonymous data is that the latter is practically impossible to be tracked back to the original subject while the former, albeit reducing the risk of identification, can still provide the possibility of a reverse compilation.

2.2.4 The notion of data-subject

The data subject qualifies as any natural person whose data have been processed. In other words, the data-subject is a person who can be identified, directly or indirectly, via an identifier. The explanation of this notion does not require excessive effort as it seems an intuitive concept.

It is important to notice that there are some specific categories of data-subject who, due to their particular vulnerability, are specifically protected under the GDPR. See, in this respect, recital 76, where the Regulation recognizes specific level of protection to data-subjects according to «the likelihood and severity of the risk to [his or her] rights and freedoms». Recital 75 further specifies this risk-based approach, affirming that the specific vulnerabilities of each data subject, in particular children, are to be duly considered.

2.2.5 The notion of data-controller

In order to correctly apply the data protection framework (and, as we will explain later, especially the principle of accountability) it is necessary to properly understand the different roles of the various agents that are involved when personal data are processed[16].

According to the EU Commission, data-controller is the entity that decides about the "how" and the "why" of the processing. In other words, the data-controller is identified as the person who determines the **purpose** and the **scope** of the processing.

Accordingly, if the decisional power is shared by two or more entities, they become **joint controllers.** In the pursuit of compliance with GDPR provisions, the joint controllers must set out their respective responsibilities in a clear and specific manner (e.g. entering into an agreement). The agreement between the joint controllers must give precise indications about the allocation of responsibilities. In particular, a clear division of their respective duties to provide the information referred to in art. 13 and art. 14 of GDPR is required. In other words, they have to determine, in a transparent manner, their respective responsibilities for compliance. The themes where this clarification is needed the most are the duty to ensure to the data subject an effective possibility

[15] Recital 26, Reg. EU 679/2016

[16] Article 29 Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169)

to exercise his or her right and the duty to provide the information listed in art. 13 and in art. 14 of the GDPR (Reg. EU 679/2016).

The role of data controller is not fixed and it changes accordingly to concrete circumstances at stake. As soon as the data-controller loses control over scope, purpose and means of the processing, he loses his title. Not differently, when another subject acquires such power, he is automatically entitled to the qualification of data controller.

2.2.6 The notion of processing

Processing means any operation performed on personal data. The notion of processing is particularly wide. The notion of processing includes, but it is not limited to: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (art. 4.2 of GDPR)[17].

2.3 Data protection principles (applicable to SUCCESS Solutions)

According to the GDPR (Reg. EU 679/2916), these principles apply whenever personal data are processed. Compliance with these principles is fundamental.

2.3.1 The principle of lawfulness, fairness and transparency

Under art. 5, par. 1, lett a) of the GDPR (Reg. EU 679/2016), personal data shall be processed «lawfully, fairly and in a transparent manner». Accordingly, it is possible to divide this principle in three sub-principles:

- Lawfulness: that is to ensure that the processing complies not only with the GDPR but also with other pieces of European legislation. It also requires that the processing of data is carried out on one of the legal bases listed in art. 6 of the GDPR (see subsection 2.2.1.1).
- Fairness: that is to ensure that, beyond formal compliance with the law, data-controller processes data in good faith.
- Transparency: this principle means that the data-controller must inform the data-subject about the processing performed on his data, clarifying e.g. what information has been collected about them, the purpose of its use, who can access and use it, the period for which the personal data will be stored, and the existence of a profiling technique. Compliance with this principle also requires that the data-controller informs the data-subjects about their right (and how to exercise them). Among the rights of data subjects, we find the right to withdraw consent, the right to be informed about the processing, the right of access, the right to data rectification, the right to erasure, and right to data portability.

2.3.1.1 Legal basis for processing

The principle of lawfulness is strongly related to the concept of **legal basis**. Under art. 6 of the GDPR (Reg. EU 679/2016), personal data can be processed only when at least one of the situations listed in art. 6 occurs. The processing of personal data can take place when:

- The data subject has given consent to the processing;
- The processing is necessary for the performance of a contract to which the data subject is party;
- The processing is necessary for compliance with a legal obligation to which the controller is subject;
- The processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest
- The processing is necessary for the purposes of the legitimate interests pursued by

[17] The data controller – processor (see definitions below), needs to determine if at least one of these operations is implemented and to what extent its organization has control on this.

the controller

It is important to specify the requirement of “necessity”: processing is considered to be necessary when the purpose of the processing (e.g. contract, legitimate interest, etc…) cannot be achieved by some other reasonable means.

In art. 6 the legal bases are not mentioned according to a hierarchical criterion: no legal basis can be considered better than the others. Simply, the choice of the most appropriate legal basis is to be carried out by taking a close look at the circumstances at stake, the purpose of the processing, and the relationship between the data-controller and the data-subject.

However, given their relevance in smart grid environments, specific attention will be given to the analysis of (a) the consent of the data subject, (b) the performing of a contract and (c) the legitimate interest of the data controller.

a) The consent of the data subject

Consent is described as an affirmative act expressing unambiguous indication of the data subject's agreement to the processing of their personal data. In the words of the WP 29[18], consent «must always be given through an active motion or declaration» so to make «obvious that the data subject has consented to the particular processing[19]». The necessity for a deliberate action means that the data-controller has to check whether the data subject is conscious of what he is consenting to. As a consequence, silence or inactivity (e.g. use of pre-ticked opt-in boxes) cannot be considered as a form of consent.

Accordingly, consent must present, cumulatively, specific attributes[20]

It must be:

- **Unambiguous** and explicit;
- **Freely given,** in the sense that it should be the result of free choice and effective control. For example, the consent given as a non-negotiable part of terms and conditions or given in a situation of *strong imbalance of power* is not considered *freely given*;
- **Specific,** this meaning that the data-subject has to consent to one or more specific purposes, so that the generic consent for any later defined purpose will not be compliant with the GDPR.
- **Informed,** so that the data-controller must give to the data-subject a set of information (e.g. the controller’s identity, the purpose of processing). The information is to be given in a clear and accessible form (e.g. not hidden in general terms and conditions) and calibrated on the specific feature of the data-subject, so as to ensure that everyone can effectively comprehend what they are consenting to.

It is also necessary to remember that, according to the principle of accountability, the data-controller should be able to demonstrate that the consent of the data-subject respects all the requirements listed above.

If consent is withdrawn, the data controller has to stop immediately the processing of personal data, albeit the operations carried out before the withdrawal remains valid. The data controller can keep processing the personal data collected under the consent if the further processing is permitted on another legal basis.

Given the importance of **consent** and **the way it will be obtained**, see specific ANNEX II on **Consent forms in SUCCESS**.

b) The performing of a contract

[18] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 679/2016 (28 November 2017).

[19] *Ibid.*

[20] Art. 7, Reg. EU 679/2016.

This legal basis of contract can be activated when the data controller is processing data for the performance of a contract that cannot be carried out by any other reasonable mean or when the processing is required in order to enter into the contract. In both cases, the requirement of "necessity" means that if there is another reasonable mean to achieve the same purpose, than this legal basis cannot be used.

c) The legitimate interest of the data controller

It is not difficult to note that the legal basis of "legitimate interest" is the most flexible one. Being an open clause, it is applicable in a wide range of situations, easily adapting to the circumstances at stake. According to the Information Commissioner's Officer (ICO), the legitimate interest of the controller is the appropriate legal basis when the processing 1) is not required by law, 2) has a clear benefit on the data controller, 3) has a limited impact on the privacy of data-subjects, 4) is a reasonable and predictable use of those data. Obviously, this legal basis is incredibly more advantageous for the data controller as he or she does not have to rely entirely on the possibly changing wishes of the data-subject, who is free to withdraw consent at any time.

However, it is undeniable that the vagueness of the concept of "legitimate interest" if, on the one hand, permits a flexible application, on the other hand it is the factor making its detectability difficult. This difficulty in finding a precise definition and a reliable criterion to assess its applicability is demonstrated by the GDPR itself. This notion, in fact, is not defined but rather explained through examples. In particular, an exemplificative list of situations where the possibility to use the legitimate interest of the data controller as legal basis are: direct marketing purposes, preventing fraud, processing employee or client data, intra-group administrative transfers.

Obviously, there are appropriate safeguards:

- The data controller must carry out a "balancing test", with the aim of checking whether the interests or the fundamental rights and freedoms of the data subject are not overriding the legitimate interest of the data controller.
- The data-controller can use the legitimate interest as legal basis only to the extent to the data-subject could have reasonably expected the processing. Otherwise, the legitimate interest of the data controller is not likely to pass the "balancing test".

2.3.2 The principle of purpose limitation

This principle requires that data are «collected for specified, explicit and legitimate purposes». Accordingly, at the moment of data collection the data subject must be informed about the purpose pursued by the data controller, this meaning that those purposes must be clearly determined at the moment of collection and notified to the data-subject. Moreover, it is not possible to further process data in a manner that is incompatible with the purpose initially declared. Processing data for a purpose that is different from the initially declared one is forbidden.

However, at certain conditions, it is still possible to process data for a different purpose. According to EU Commission, when the legal basis (see subsection 2.2.1.1) is not the consent of the data-subject, the processing is permitted as long as the new purpose is **compatible** with the originally declared one, within the original legal basis (unless the original legal basis was consent). The elements that should be taken into consideration in order to carry out the **compatibility test** are:

- The link between the original purpose and the new/upcoming purpose;
- The context in which the data was collected, in the sense of consenting a change of purpose when it is possible to believe that, thanks to the context of collection, the secondary purpose could have been reasonably predicted by the data subject.
- The type and nature of the data (is it sensitive?);
- The possible consequences of the intended further processing (how will it impact the individual?);
- The existence of appropriate technical safeguards (e.g. pseudonymisation).

2.3.3 The principle of data minimisation and storage limitation

According to the **data minimisation principle**, information systems and software shall be configured in order to minimise the processing of personal data. This means that only data that are «adequate, relevant and limited to what is necessary in relation to the purposes of the processing» can be collected and further used by the data-controller. As will be pointed out later, this principle is particularly relevant in the context of smart grids.

Similarly, the principle of storage limitation requires that data are stored «for no longer than is necessary for the purposes for which the personal data are processed», meaning that when data are no longer needed according to the purpose of their collection, they must be erased or, at least, anonymised.

2.3.4 The principle of accuracy

Under art. 5, par. 1, lett. d) of the GDPR (Reg. EU 679/2016), the principle of **data quality** requires that data are «accurate and, where necessary, kept up to date». This principle protects both the interest of data-controllers (so to avoid misrepresentation of the matter of fact which may result in a mistaken outcome of the processing) and data subjects (so that their identity is not falsely represented). Accordingly, the data-controller should set up all the measures that are necessary to rectify or erase false or outdated data.

2.3.5 The principle of integrity and confidentiality

Those principles are particularly relevant in the context of secure smart grid as they are deeply connected with cyber security. According to art. 5, par. 1, lett f), the data controller should set up adequate safeguards, both technical and organisational, in order to protect data «against unauthorised or unlawful processing and against accidental loss, destruction or damage».

2.3.6 The principle of accountability

The concept of accountability is particularly difficult to explain. Basically, data controllers are required to set up all the technical and organisational measures not only to comply with the principles and the other legal obligations of the GDPR but also to give proof, when requested, of the precautions adopted. The GDPR (Reg. EU 679/2016) puts forward a non-exhaustive list of instruments to be used for such purpose: the Records of processing activities (art. 30), the data protection impact assessment (art. 35), codes of conduct (art. 40) and certifications (art. 42).

3. Privacy-by-design solution in SUCCESS

The following paragraph is a brief summary of the **privacy-by-design solutions** elaborated in the context of SUCCESS. According to the purpose of this deliverable, they will not be explained in details. The technicalities of the privacy-by-design solutions specific to the SUCCESS project, in fact, are not in the scope of this deliverable, which is rather directed to the *general* audience of entities acting in the context of smart grids and privacy. The data protection principles (chapter 2) and guidelines/best practices (chapter 4), far from being applicable in the sole SUCCESS context, apply to all the privacy-related issues of smart energy distribution. For the details of the privacy-by-design measures elaborated in particular for the context of SUCCESS, please see. D. 4.10[21].

Accordingly, a bullet-pointed list of the solutions implemented in SUCCESS follows. They will be used in this deliverable as basis to develop the more general guidelines and best practices that will be explained in the following chapter (chapter 4):

- **Anonymisation of data at the utility level** which, according to the *relative* and *subjective* notion of anonymity (see subsection. 2.1.2), operates a process of *de-personalisation* of data before they leave the user-level;
- A **Role Based Access Control System (RBAC)** which is used in order to permit to end-users to decide which kind of subjects (based on their roles) can access their data, when, how, and how long. This is consistent with the *principle of transparency* (the data subject is perfectly aware of who can access his data) and with the aim of guaranteeing him/her a minimum threshold of *control on the processing* of his/her personal data;
- **The sharing just network data[22] (and not consumption data[23])**, so as to impede the flow of personal data beyond the utility level;
- **A "database centric architecture"**[24], which is used in order to impede any access by external actors without passing through the central database of NORM. The access to the central data base of NORM can be done exclusively through a MQTT-based interfaces implementing RBAC;
- **A system permitting the access by the DSO only to specific data, after the consent of the end-user**. This is necessary in order to comply with data-minimisation principle and to guarantee to the end-user a minimum threshold of control on his data;
- **A way to secure the communication with the DSO and also with all others actors** (e.g. ESCO or energy supplier): the communication of data is made with the specific DSO using VPN and the whole SCADA application is sandboxed in a Docker cluster containing an MQTT broker, the SCADA app with IEC61850 protocol, and the VPN client;
- **A "User Privacy Profile" UPP** System, which provides the right of data access for any specific qualified actor within the SUCCESS Components**.** This measure is adopted in compliance with:
    - Specific National rules about smart grids maintenance and public security rules in the energy sector,
    - Specific instructions given by the end-users through its UPP,
    - Data protection framework, in particular art. 6 of the GDPR (Reg. EU 679/2016);
- **"SMXCore"**[25], a Open Source/Open Access MQTT oriented platform, which is used in order to provide each end-user (data subject) with the possibility to access his or her own specific user account on this platform. On this platform it is possible to:
    - Access all personal data (user's data, e.g. energy consumption data),
    - Allow and deny accesses to Privacy Profiles,
    - Rectify some data that he has previously provided to the DSO (e.g. identification data like name, fiscal code, building information, etc.),

[21] Deliverable 4.10, Innovative approach to data privacy for energy services

[22] Network data are data concerning the functioning of the grid, as a whole. Those data do not regard single users.

[23] It is important to highlight that from network data it is not possible to infer consumption data.

[24] See Deliverable 3.7, Next Generation Smart Meter, SUCCESS - Securing Critical Infrastructure, Forthcoming 2017, Section 4.

[25] available at this site: https://github.com/SMXCore/SMXCore_NG

    - Read purposes and any other meaningful information about the processing of data (according to art. 15, GDPR),
    - Control the flow of his personal data through the platform;
- **The possibility to exercise the right to erasure and the rights to portability** through a specific request to the Data Protection Officer of the DSO;
- **The possibility for NORM users to define a specific time period when data can be shared.** Accordingly, it is "by-design" possible to pre-set the period of the data flow from NORM to DSO or other eventual subjects or components of the smart grid system;
- **A "double virtualisation" system**, composed by a data-layer (where all personal data are stored) and a functionality-layer. Those layers are totally separated. This is a form of data minimization and it potentially enhances disaster recovery. In case of attack targeted at a single layer, its effectiveness will be reduced as the other layer will not be affected and all the relevant entities will be migrated to the other layer;
- **A Double Virtualization (DV) technology,** a mechanism for the backup of both grid and functionality data.

3.1 Three-step DPIA

Due to its importance in the context of privacy-related SUCCESS issues, specific relevance will be given to the system used in order to carry out a DPIA.

As the DPIA Smart Grid Template clarifies, a DPIA should be executed **from the start of the design throughout the design and implementation phases**. This enables a privacy-by-design approach guaranteeing that potential risks are identified and that appropriate controls can then be built into the systems.[26]

As the GDPR points out (art. 35 Reg. EU 679/2016) Timing is an essential element to consider when carrying out a Data Protection Impact Assessment. This is why there should be at least **3 DPIAs in a project design**. In particular in SUCCESS we had three steps:

1. The first step has consisted of delivering recommendations for designers and stakeholders involved in the Architecture design in month 6;[27]
2. The second step has consisted of an intermediate Data Protection Impact Assessment that has taken into account the state of the architecture design before its completion in month 12;[28]
3. The third step has consisted of the final Data Protection Impact Assessment after that the technology has been implemented, in month 24.[29] This final DPIA was performed during months 22-24, just before the end of the project. This pre-final timing allowed the partners to take notice of the Assessment and eventually change final details of SUCCESS Components accordingly.

[26] Expert Group 2, *Data Protection Impact Assessment Template for Smart Grid and Smart Metering*, cit., p. 18.

[27] See SUCCESS Deliverable 2.1 (and Deliverable 3.1).

[28] See SUCCESS Deliverable 3.2.

[29] See SUCCESS Deliverable 3.3.

4. Lessons from the good example of SUCCESS

Starting from the good example of SUCCESS, it is now the moment to recall all the positive elements developed in the context of this project: albeit the privacy-by-design solutions listed above have been conceived in the context of SUCCESS, their possible field of application is not limited solely to the SUCCESS context. That is why it seems consistent with the purpose of this project to try to extrapolate, from the particular *ad hoc* solutions exposed in the previous paragraph, a series of guidelines and best practices that may be useful for all the agents who have to deal with personal data in the energy sector, following an inductive scheme of reasoning.

4.1 Data in smart grids environment

As pointed out in the introduction of this work, the multi-layer approach adopted by the EU institution can be put into practice. That is why, utilizing the general definition of personal data (in the GDPR), it is useful and necessary to concretize the abstract definition by looking closer at the specific circumstances at stake. To provide a specific example of what is to be considered as personal data in the SUCCESS context and, generally, in the energy sector is the main purpose of the following section.

4.1.1 What data do a smart grid need?

Without prejudice to this general definition exposed in subsection 2.1.1, the legal scenario has to be completed by mentioning some additional **definitions specific for the energy sector,** which complete (and do not substitute) the general definition of personal data in EU Data Protection Legislation. This process has resulted in a list of data[30] to consider as personal in the context of smart grid metering systems. They include, but are not limited to:

- Household's consumption;
- Consumer registration data: names and addresses of data subjects;
- Usage data (energy consumption, demand information, and time stamps), as these provide insight into the daily life of the data-subjects;
- Amount of energy and power (e.g., kW) provided to the grid (energy production), as they provide insight into the amount of available sustainable energy resources of the data subject;
- Locally produced weather forecast – consumption prediction / forecasts;
- Demand forecast of building, campus and organisation;
- Technical data (tamper alerts), as these might change how the data subject is approached;
- Profile of types of consumers as they might influence how the consumer is approached;
- Data and function of individual consumers / loads;
- House-hold operations profile data (e.g. hours of use, how many occupants at what time and type of occupants);
- Frequency of transmitting data (if bound to certain thresholds), as these might provide insight into the daily life of the data-subject;
- Billing data and consumer's payment method

It is important to underline that when this kind of data are involved, all the principles and rules analysed hereafter apply.

4.1.1.1 "Sensitive" data

Even though this notion **may not seem relevant** in the context of **smart meter data**, examples of the use of "sensitive data" can be given even in this context. For instance, energy consumption can reveal patterns of **religious beliefs** (e.g. observing Ramadan or getting ready for morning prayers[31]) or **health data** (e.g. the use of particular medical machines or a particular sleeping

[30] 'Smart Grid Task Force 2012 - Expert Group 2 for Regulatory Recommendations on Privacy, Data Protection and Cyber-Security in the Smart Grid Environment

[31] Colette Cuijpers and Bert Jaap Koops, "Smart Metering and Privacy in Europe: Lessons from the Dutch Case"; 2013, *"European Data Protection: Coming of Age"* (Springer) .

schedule). In fact, from a detailed and extremely frequent transmission of electricity usage data it is possible to **infer and predict accurate information** about the subjective condition of the data subject. From such data it may be possible to deduce a number of details about the daily routine and lifestyle of the members of a household. For instance, it is possible to predict with an incredibly high degree of certainty their working hours, their sleeping schedule (and its irregularities, as if someone suffers from insomnia), if they watch television, which tolls or devices they usually use, if they use particular workout equipment, if they generally host other people at home, how often they do their laundry, if a medical device or a baby-monitor are in use etcetera.

Avoiding an extremely frequent and excessively detailed transmission of data is a great tool not only to reduce the risk of inferring "special categories of data" (with all the legal consequences that derive from such a qualification) but also in order to demonstrate compliance with the **data minimisation principle.** Therefore, we strongly suggest to avoid such transmissions in the context of data processing in the energy distribution sector.

As already mentioned before, these data can be processed under specific condition listed in art. 9 of the GDPR (Reg. EU 679/2016).

4.1.2 Anonymous and pseudonymised data in energy sector

As pointed out in subsection 3.1, the anonymisation of the personal data involved in the functioning of smart grids is one of the most effective tools available to the data controller in order to reach compliance with data protection law. Therefore, it is strongly advised to implement a system of data anonymisation at the utility level. **Increasing the pseudonymisation** to the whole data processing (or at least as much as possible), brings great benefits in respect of the data minimization principle and, as mentioned above, of the possibilities to successfully pass the "compatibility of purposes test". As the architecture of data protection law is, in general, built up using a "**risk-based approach**", the implementation of pseudonymisation system – and the consequent decrease of the inherent risks of processing – can help the data controller to gain more room for manoeuvre and freedom in the carrying out of the processing activities.

Anonymisation and pseudonymisation of data are also relevant with regard to compliance with the **data minimization** and **storage limitation** principle (subsection 2.2.3). In fact, when the data are anonymous no processing of *personal* data is taking place. Thus, with the aim of **avoiding any collection and use of personal data** when it is **unnecessary** for the declared purpose of the processing, those measures should be adopted whenever it is possible. Furthermore, they are also functional to prevent data-breaches to the detriment of end-users: in case of an unauthorized access to the databases containing the anonymous or pseudonymised data, no personal content would be leaked.

Finally, it is important to remember that the **limitation of the processing to the sole data that are necessary for the declared purpose** is fundamental in order to activate one of the **legal bases** of art. 6 that are different from consent.

4.1.2.1 Organisational and technical measures needed

In order to implement a data pseudonymisation system, the controller must set up some **technical and organisational measures** specific to the purpose. In the first place, the data is to be separated from its identifiers; secondly, the identifiers must be substituted by unique codes or by another recognition system; subsequently, it is necessary to create two different data-bases, one for the data content associated with the **recognition code** and one to keep trace of the connection between each data-subject and his or her unique code; finally, the data-controller has to implement a system to keep those two databases strictly separated.

The goal of anonymisation, on the other hand, can be reached, in the context of real time energy services, through **data-aggregation techniques**. This means that whenever individual level data is not required as necessary for the functionality of the smart grid system, personal data should be aggregated to the point of impeding the re-identification of the single natural person originally concerned by the non-aggregated data. For instance, a good implementation of this guideline can be aggregating data at the largest territorial level as possible without compromising the functionality of the grids.

In general it is important to remember that, whenever processing personal data, SUCCESS's operators and other operators involved in the context of smart grids in general, should consider if

it is absolutely necessary for operational purposes; if the processing is not “absolutely necessary”, it should be avoided whenever possible.

4.2 Subjects involved and the principle of accountability

Starting from the general definition of data subject and data controller (subsection 2.1.4 and 2.1.5), it is now necessary to further specify the features that characterise the role of data-subject and data-controller in the SUCCESS project and, thus, in the energy distribution environment in general.

Specifying in practice those general definitions is a fundamental step to take towards the overarching goal of compliance with the GDPR. In fact, a proper implementation of the provisions of the GDPR would be almost impossible without a **crystal clear identification of data controllers (and joint controllers) and data-subjects**. Moreover, this is also necessary in order to respect the principle of accountability, as, in the absence of a proper distinguishing between the subjects involved in the processing, a clear **allocation of responsibilities** (required under the *accountability* principle) would result impossible to put in practice.

That is why, in the context of SUCCESS, we have tried to **elaborate a practical rule** in order to from a data protection point of view distinguish the subjects involved and to properly allocate the responsibilities of the processing. However, the results of the SUCCESS project are equally valid in every context where a privacy approach to the energy distribution is necessary. Hence, in the following section, we formalised some “exportable” guidelines.

4.2.1 Data Controller, data processor and joint controllers

In general, as for the determination of the **controller**, the ***golden rule*** is that we should consider as the data controller of a particular processing the entity who determines its scope, means, and purposes. As such, they have all the **duties** and the **responsibilities** already described in subsection 2.1.5, for instance, to provide the data subject with adequate information and to set up all the technical and organisational measures needed to ensure a fair form of processing. Instead, when two or more entities share the determination of scopes and means of the processing, they will be considered as **joint controllers.** This qualification comes with the duty, as explained above, to share their duties and responsibilities clearly and precisely. With regard to the **data processor**, instead, he is defined as the entity that, in the processing, acts according to the *instructions* and under the *control* of the data controller.

Having briefly recalled the general discipline, here are some specific examples attaining to the activity of data processing in the energy sector with the aim of clarifying the role of the subjects that commonly take part in the smart grids’ functioning.

- **DSO and Energy Supplier:** determining the role of these entities can be difficult as it varies from country to country, depending on what energy distribution model the country has adopted.
    - In some models, the entity who decides the scope and the means of the processing and, thus, has the role of data controller is the **energy supplier.** This entity, in fact, **signs the contract** with the final customer, decides which data are needed for the functioning of the smart grids, how these data will be collected, stored and used. Therefore, it is evident that the scope, the purpose and the means of the processing are up to them. This establishes them quite clearly as a data controller for the processing.
    - In other countries, the **DSO**[32], when owning the smart grid, is responsible for the functioning of the smart grids. Therefore, the DSO will also be in charge of the determination of the modalities of collection, usage, and storage of the personal data that are necessary for the functioning of the smart grids. He will also take decisions concerning the finalities of the processing and the appropriate safeguards. Obviously, the DSO can outsource parts of his metering business to

[32] According to art. 2 n. 6 Dir 2007/72/EC, the Distribution system operator (DSO) is a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long term ability of the system to meet reasonable demands for the distribution of electricity.

a data processor (e.g. reading out meters, delivery of meter data, etc.).
  - Obviously, sometimes it is possible to consider the DSO and the energy supplier as **joint controller**. This can be the case of the situation described under lett. b) of this list (DSO as responsible for the functioning of the smart grids), where the energy suppliers are entitled to access the personal data transmitted by the meters in order to use them for his own purposes.
  - The **DSO** can also be considered merely as **data processor**. For example, this could be the case if it acts only on the instructions of the suppliers to and from whom it sends and receives data. This happens when the model is conceived so that the central communication function (the transmission of data between the meter and the supplier) is a task of the DSO. On the contrary, he can be considered a data controller when his function of data communication, going beyond the mere execution of the instructions by the energy supplier, includes also the decision about whether personal data can be disclosed to a third party or whether such data can be processed for new purposes.
  - In most member states, there is a sort of **hybrid situation**: the DSO is the metering operator and as such, the DSO is the data controller in the first part of the metering data process. The DSO's processing ends with the creation of a bill for the network usage. Subsequently, the energy supplier becomes competent to determine the scope, the purpose and the means of the processing and, as such, he is considered data controller. In this moment, in fact, the energy supplier is provided with the personal data collected by the DSO in the first step of the process, so that he can create, with those newly acquired data, a bill for the electricity supplied.

- **Cloud service providers for smart data back-up:** when the functioning of the smart grid implies a disclosure of data to a third party, such as a cloud service provider, the entity will assume the role of a *data controller* or, when the control of the processing (in this case, the storage of data) is shared with another entity, then it will assume the role of joint controller.
- **Prosumers:** Being the final customers of the real time energy service, prosumers are typically considered *data subjects.* However, it is thought that they can assume the role of joint controllers, when their activity goes beyond the "purely personal" level. For instance, such a role can be recognised to landlords or, more in general, to people who host guests in their houses for commercial purposes (AirBnB, B&B, rental) or who earmark their property for professional activities.

4.2.2 Data subject

As said, the data subject is the **natural person** whose personal data are processed. In the context of smart grids, it is generally said that the data subject is the end-user of the service. Based on this general rule, it is also necessary to remember that, **in the case of prosumers,** it is possible to consider end users as joint controller, as mentioned above.

4.2.3 The importance of a clear division of roles

The clear distinction of the roles of people involved in the data processing is absolutely necessary, as already pointed out, in order to comply with the **principle of accountability.** In fact, in order to comply with this principle, it is necessary to clearly distinguish among the subjects that are involved in the processing, so that everyone can be held accountable for the responsibilities connected with his role. Furthermore, this principle requires not only that the data controller and the data processor respect the duties provided by the law, but also that they are able to demonstrate their compliance. That is why, on the basis of the SUCCESS experience, we strongly recommend to any of the operators working in the context of smart grids to have a **precise notion of his roles, duties and responsibilities**.

Moreover, a full understanding of who is the data controller is fundamental, especially in the context of the energy distribution, in order to be able to ground the processing on the most appropriate **legal basis**. As mentioned above, there is no clear line between the various legal bases and the risk of overlapping is incredibly high. Due to the fact that the features of the **relationship between the data subject** (the end-user) **and the data controller** (the DSO or the

energy supplier) are specifically listed among the criteria used for the choice of the most appropriate legal basis, a clarification on who is the data controller is absolutely necessary.

4.3 Processing activities in smart grids environment

The non-exhaustive list below provides some illustrative examples of **processing of personal data in smart meter environments**:

- **Reading out** a meter manual/remote or **collecting/storing** data in a database;
- **Storage** of meter data in meter or telecommunication device including "intermediate storage" (e.g. cloud providers);
- **Transfer** of meter data via WAN to a back end system.

4.3.1 A particular kind of processing: transferring data outside the EU

When a data controller decides to transfer data **outside the European Union**, he needs to comply with a strict set of rules. In fact, there is no certainty that countries outside the EU have adequate data protection legislation. Therefore, this particular processing is likely to expose the data-subject to greater risks than if their data had remained inside the EU. The degree of protection established by the GDPR, in fact, is higher than the average legislation of other countries.

Whereas at the current state there is no need to carry out such an operation in the context of SUCCESS, according to the purpose of this paragraph (giving **advices generally valid** to accomplish an adequate degree of privacy in the energy sector, in spite of the peculiarities of the specific circumstances at stake), we will list the additional safeguards that should be set up if it happens to be the case. Furthermore, even if not strictly necessary, it is not unlikely that also the SUCCESS project, sooner or later, employs instruments such as software, online services, and clouds from service providers based outside the EU. In such a case, the following provisions must be taken into consideration.

Under **art. 45 of the GDPR (Reg. EU 679/2016), «**A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection».

In other words, the Commission is tasked to evaluate whether the third country at issue is able **to ensure an adequate level of privacy of the end-user and data protection**. Essentially, the decision aims to check whether the laws of the third country are able to provide a level of personal data protection that is almost equivalent to the degree of protection inside the EEA If the evaluation (so-called "**adequacy decision**") **of the Commission** is not in favour of the data transfer, **the data controller** can still decide to carry out the transfer. However, he is requested to provide appropriate safeguards and countermeasures, otherwise the transfer will not be GDPR compliant. The exemplificative list of **safeguards** provided by recital 108 and art. 46 of the GDPR includes, but is not limited to:

- Legally binding and enforceable instrument between **public authorities**;
- Binding corporate rules;
- Standard **data protection clauses** adopted by the Commission or by a supervisory authority but still approved by the Commission;
- Approved code of conduct;
- An approved **certification** mechanism.

Another **compulsory condition** for the transferring of data in the absence of a positive outcome of the evaluation of the Commission is the availability of «**enforceable data subject rights** and effective **legal remedies** for data subjects[33]».

Imagining the **worst-case scenario**, where neither the country provides adequate safeguards, nor the controller ensures the required safeguards**,** the transfer of personal data to third countries

[33] Art. 45, Reg. EU 679/2016

can take place only if **additional conditions**[34] are met.

Among these we selected and list the three situations that are most relevant in the context of real time energy services:

- The transfer is necessary for the **performance of a contract between** the **data subject and the controller** or the implementation of **pre-contractual measures** specifically requested by the data subject;
- The transfer is necessary for the **conclusion or performance of a contract** between **the data controller and another entity of the third country**, as long as this contract is concluded in the interest of the data subject;
- The data subject has given his **explicit consent** to the transfer. Obviously, the consent must be informed, this meaning that the data subject has to be perfectly aware of the risk that the processing at issue can pose to his or her own rights and freedom and must have specifically accepted them. As a consequence, it is necessary to explain to the data subject whose personal data are about to be transferred that such transfer is to an area where EU rules on data protection do not apply, being the country outside of the EEA.

Here, a disclaimer is needed: after ***Brexit***, England is a fully-fledged "third country". This means that the transferring of data to entities that are located in Britain should comply with the provisions set out above. However, there is a constant cooperation between the ICO and other Data Protection Authorities across the EU and the government declared that UK is willing to sign an agreement on data protection with the aim of gaining an "**adequacy decision**" from the Commission[35].

4.4 Processing metering-data: which legal basis?

As already pointed out, the **legal bases** outlined in art. 6 are not sorted according to a hierarchical criterion. The data controller, has to choose the most appropriate legal basis according to the peculiarities of the specific circumstances at stake. For instance, as already explained in subsection 2.2.1.1, one of the criteria to determine the most appropriate legal basis is the relationship between the data controller and the data subject.

Therefore, considering the scenario of data protection in energy distribution, we have identified **three legal bases** that can be useful in the energy distribution context.

4.4.1 The performance of a contract

The data controller can rely on this legal basis in two cases:

- When the data processing is necessary **to meet the contractual obligations** the data controller entered into, in the sense that the processing of data is essential to comply with your obligations as part of that contract.
- When the data processing is **functional to the conclusion** of the contract, in the sense that the data controller, not having a contract with the data subject, is asked to do something as an initial step functional to the closing of the contract.

It comes without saying that the possibility to use this legal basis is strictly connected to the **necessity of the purpose of fulfilling the contractual obligations.** In fact, if there are other

[34] Among the conditions of art. 49, the most relevant in the energy sector context are: a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.

[35] "UK stands by 'adequacy-plus' Brexit data protection proposals" in *outlaw.com,* 13 luglio 2018. accessed 25 sett. Available from: https://www.out-law.com/en/articles/2018/july/brexit-uk-adequacy-plus-data-protection-/

reasonable ways (not implying the processing of data) to fulfil the contractual obligation, then the "contract legal basis" cannot be activated.

Focusing the attention on the **energy distribution activity**, it is easy to notice that this legal basis is pretty easy to activate when the data controller is the energy supplier (this entity, in fact, signs a distribution contract with the final customer/ data subject). That is why we strongly recommend the utilization of this legal basis when the data controller is the same entity who has concluded the distribution contract with the final customer (data-subject).

However, having said that **"necessity" is a mandatory feature** of the data that the controller decide to process within this legal basis, it is compulsory for the data controller to fully respect the principle of data minimization. As a consequence, it is strongly advised that, in this case, the data controller (that is the energy supplier) carefully chooses which data are absolutely essential to the processing.

4.4.2 The legitimate interest of the data controller

This legal basis can be considered the most "flexible" of the legal bases provided by the GDPR. It can possibly be applied to any kind of processing as long as it is carried out for a reasonable and fair purpose[36]. The flexibility of this legal basis is sufficient in order to consent its usability in both the models described in subsection 4.2.1. Nevertheless, we suggest using this legal basis mainly in those contexts where the data controller is the DSO. The DSO, owning the smart grid, is responsible for their proper functioning. Accordingly, it is undeniable that the interest that the controller (the DSO) has in the processing is to maintain the maximum functionality of the smart grid. There is no doubt that the processing of data for the purpose of functionality of the grid itself can be considered a legitimate interest of the DSO.

To in practice assess the presence of a legitimate interest, the data controller has to answer a number of questions, easily summed up in the combination of:

- The "**purpose test**" (why do you want to process the data? What are you trying to achieve? Who benefits from the processing?);
- The "**necessity test**" (Is the processing necessary for that purpose? Does this processing actually help to further that interest? Is it a reasonable way to go about it?);
- The "**balancing test**" (do the data subject's interests override the legitimate interest? What is the nature of your relationship with the individual? Would people expect you to use their data in this way? What is the possible impact on the individual?).

4.4.3 The consent of the data subject

Whereas a number of data processing is carried out on this basis, according to a number of experts, **the consent of the data subject is the weakest legal basis.**

In fact, the use of consent as legal basis for the processing has a number of disadvantages:

- It **impedes the possibility to change the purpose** of the processing, even when compatible with the purpose initially declared
- It is **continuously at risk of withdrawal**, so that it is not impossible, for the data controller, to be forced to immediately stop the processing.

Furthermore, in the specific case of smart grids, we believe that consent is not the appropriate legal basis due to the peculiarities of that specific processing. Some voices, have pointed out that there are some doubts concerning the qualification of the consent given by user of services whose functionality is strictly dependent on the processing of their personal data as «**freely given**»[37]. The data subject, in fact, cannot «**refuse or withdraw** consent **without detriment**»: the refuse

[36] Moerel Loekke, "GDPR conundrums: Processing special categories of data", IAPP, 2016, p. 44. Available from: https://iapp.org/news/a/gdpr-conundrums-processing-special- categories-of-data/. Accessed: 24 April 2018

[37] Eskens Sarah, "Profiling the European consumer in the Internet of Things: how will the general data protection regulation apply to this form of personal data processing, and how should it?", 2016, p. 19. Available from: https://ssrn.com/abstract=2752010. Accessed: 5 April 2018.

or the withdrawal of the consent, could seriously damage the functioning of the smart grids, resulting in a clear «detriment» to the final customer[38].

In addition, when the legal basis is consent, it is not possible to change the purpose of the processing through the "compatibility test".

For all the reasons listed above, it would be **better to rely on a legal basis different from consent**. Obviously, according to the purpose of this paragraph, this advice is equally valid not only for the SUCCESS project but also, more in general, for the whole sector of energy distribution.

4.5 A final disclaimer: secondary uses and compatibility of purposes in smart grid-security system

This last problem is particularly relevant in smart-grid-security systems (similar to the one developed by SUCCESS). It is not unlikely for the data controller of this system to develop, at a later stage of the processing, the **subsequent need** to process personal data for further purposes, different from the purposes declared at the outset of the processing and approved by the data subject. For instance, in the event of new threats or new and innovative security techniques emerged after the obtainment of consent to the processing of data by the end-user.

If the data controller has used consent as legal basis to start the processing, then some limitations apply:

- To change the purpose of the processing he is required to submit another **specific request** for consent to the data subject, as the utilisation of consent as legal basis impedes the application of the provision concerning the compatibility of purposes.
- It cannot be **swapped** to another legal basis. In this case, a "new" processing has to start.

As asking new consents from customers is somehow inefficient in terms of security and sustainability, it would be better to avoid the use of consent as legal basis. In fact, when consent is not involved, it is always possible to change the purpose of the processing after the positive outcome of the "**compatibility test**".

As we already mentioned, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, the controller should take into account a number of factors. Here, focusing on the context of smart grids, we would like to select, from the general list of art. 6, par. 4, the items that are most relevant in the context of SUCCESS:

- The provision of art. 6, par. 4, lett a) considers as relevant for the "compatibility test" any **link between the purposes** for which the personal data have been collected and the purposes of the intended further processing. The importance of this provision can be stressed in particular when the data are collected for a reasonable purpose.
- Under art. 6, par. 4, lett b), instead, **the relationship** between data subjects and the controller is a factor to take into consideration when evaluating the change of purpose.
- Lett. e) of the same article, instead, is focused on the existence of appropriate **safeguards**, which may include encryption or pseudonymisation. This is particularly relevant for the SUCCESS project: pseudonymisation can easily be implemented for most processing.

For all the reasons listed above and given the delicacy of the matter at hand, it is highly recommended that, both in the context of SUCCESS and in the general environment of energy distribution, the purposes and contents of the processing are identified to the **largest extent possible** in order to reduce at the minimum the inherent risk of not complying with the purpose limitation principle.

[38] Helberger Natali, "Profiling and targeting consumers in the Internet of Things: a new challenge for consumer law", 2016. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717. Accessed: 5 April 2018

4.6 DPIA in smart metring context

The DPIA is a strong suit of the SUCCESS project. As already pointed out, during SUCCESS, the elaboration of the DPIA took place in three different stage: in the first place, **recommendations** were delivered for the architecture and to the designer in charge of design; subsequently, an **intermediate DPIA** took place, so as to evaluate the architecture design before its completion[39]; finally, after the final implementation of the technology, the **final DPIA** was released before the end of the project so as to allow the partners to take notice of the results of the Assessment and eventually change final details of SUCCESS components accordingly.

The SUCCESS project strongly encourages the extension of such a procedure to other projects in the field of energy distribution. These **continuous DPIA** have proved to be extremely effective in a context where there is the necessity to adapt quickly to the evolution of the circumstances at stake. The DPIA is not a static document and is to be continuously adjusted during the running of a project, especially in a situation where the privacy risks are continuously changing.

4.6.1 The DPIA: practical suggestions

Obviously, the DPIA must be compliant with the **guidelines** elaborated by the EU Commission together with the opinion issued about them by the WP 29[40].

We believe that a discussion on those guidelines would be useful not only to the SUCCESS project but also to other smart grid operators. The document issued by the Commission, in fact, is addressed to a **broad audience** (Transmission System Operators, Distribution System Operators, Energy Generators or Producers, Energy Market Suppliers, Metering Operators, Energy Service Companies) so that, according to the aim declared at the beginning of this paragraph (that is not to limit the benefits deriving from the SUCCESS project to the sole SUCCESS context), we decided to here recap some of its most relevant points, for the **benefit of the whole energy distribution sector**.

The DPIA test must be executed following these steps[41]:

- **Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA.** This step is necessary in order to decide whether a DPIA is needed or not. This decision should be inspired by a number of different criteria, such as the personal data involved (e.g. whether they are “sensitive” or not), the expected impact on rights and freedom of the data-subject, the possible public concern, the nature of the smart grid system or application;
- **Step 2 – Initiation.** This step is directed to set up the appropriate organisational measures for the positive outcome of the DPIA. Some specific measures (concerning e.g. the DPIA team or the resources needed) are taken in consideration:
- **Step 3 - Identification, characterisation and description of smart grid systems or smart grid applications processing personal data.** This step requires a comprehensive and full picture of the application of the smart grid system, its environment, the processed data and system boundaries;
- **Step 4 - Identification of relevant risks.** This step aims to identify the potential risks that may threaten the data subject and impact his or her privacy (illegitimate access to data, unavailability of legal processes, etc.), and to recognise the source of such risks (insider, outsider, machine);

[39] See SUCCESS Deliverable 3.2.

[40] Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid andSmart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force (WP 209); Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force (WP 205).

[41] For further information on this topic, we suggest to visit: https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

- **Step 5 - Data protection risk assessment.** This step aims to evaluate the risks identified in step 4 according to a severity and likelihood criterion;
- **Step 6 - Identification and recommendation of controls and residual risks.** This step aims to present the controls that have been implemented or are planned to be implemented in order to reduce risks. The commission strongly advise the consultation of the BAT (Best Available Techniques) elaborated by the Expert Group 2;
- **Step 7 - Documentation and drafting of the DPIA Report.** This step is focused on the drafting of the final DPIA report. An accurate documentation of the steps listed above should be presented in the final DPIA report. This report can be distributed to stakeholders;
- **Step 8 - Review and maintenance.** This step looks at the dynamic dimension of the DPIA. The periodical need for revising is to be taken into consideration, especially when the technologies available are quickly evolving.

4.7 A call for standards

As we can notice, the field of smart metering is characterized by strong difficulties in setting clear standards and good practices. Such an operation, instead, would help the DSO and the Energy Supplier (as data controller) to have a clear idea of the best practical implementation of their legal obligations and, as a consequence, this would also permit the end-user (as data subject) to reach an effective and full enjoyment of his or her rights.

That is why, with the aim of providing more clarity and certainty of the legal background, we decided to sum up some of the most relevant non-binding documents available at the moment: the Guidelines from the WP 29, and the Guidelines from NIST and the BTA from the EU Commission. We believe that even if carried out in the specific context of the SUCCESS project, such an operation could bring enormous advantages to the whole audience of the stakeholders involved in the functioning of smart metering systems.

4.7.1 Guidelines from the WP29 and NIST

From the comparison of the Opinion on Smart Meter issued by the WP 29 (Art.29 WP/183)[42] and the guidelines for smart grids cyber-security by the U.S. NIST[43] we extracted some basic principles and practical tips to help the data controller in the implementation of privacy-enhancing systems in the smart metering context.

Accordingly, here we have included a **summary** of the points stressed the most by these two bodies:

- Personal information in all forms should be protected from **unauthorized modification**, copying, disclosure, access, use, loss, or theft;
- **Unauthorised disclosures** of personal data must be avoided at all costs, e.g. through a system monitoring all data access or a system for the authentication of the identity of any recipient of personal data. Information should only be used or disclosed for the purpose for which it was collected and should only be **divulged to those parties authorized to receive it**. Personal information should not be disclosed to any other parties except for those identified in the notice;
- The **maintenance of data integrity** to protect against unauthorised modification, e.g. through a system to monitor all data modification. The avoidance of important services being disrupted due to attacks on the security of personal data;
- The **minimisation of the personal data used**, e.g. the aggregation of data whenever individual level data is not required, collection only of the personal information that is required to fulfil the stated purpose; storage of the information for only as long as is necessary to fulfil the purposes;

[42] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering (4 April 2011).

[43] U.S. NIST, “Guidelines for smart grid cyber security (vol. 1 to 3),” NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

- The **constant and detailed information of the data subject**, e.g. through a clearly specified notice about the purposes and the manners of the processing;
- The **highest degree of freedom** of the data subject as possible, for instance through the presentation to the users of various choices for the processing of their data and through the provision of privacy policies to the service recipients;
- The **enforceability of the rights and freedoms** of the data subject, for instance giving the possibility to **challenge an organization's compliance** with the legal framework and with their own declared policies.

Given the **positive outcome of the practical implementation** of these practical advices in the context of this project, we strongly suggest the extension of them to the whole energy distribution sector where dealing with personal information of the service recipients.

4.7.2 The BTA (Best Available Technologies) in Smart Metering Systems

Focusing the attention on the technical measures to implement, there is not a clear idea of what actually constitutes an acceptable threshold of privacy and data protection in smart metering systems or applications. As a consequence, according to the suggestion by the EU Commission[44], a **Stakeholder Forum** was created. Their work resulted in a document[45] elaborated by the *Smart-Grid Task Force*. This initiative seeks to assess the Best Available Technique assessment, so as to reorganise and clarify the legal and technical background of smart metering systems.

The document issued identifies and selects the "**Best Available Techniques** (BAT) **for the 10 common minimum functional requirements related to the Smart Metering System roll-out under a Cyber-Security and Privacy Perspective**". The EU Commission[46], in the 2012 Recommendation, defines the BAT as «the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU data protection framework. They are designed to prevent or mitigate risks on privacy, personal data and security».

Such an operation was necessary also for consenting an **easier compliance** with the accountability principle: the lack of clarity about the techniques whose implementation is advised in order to mitigate the inherent risks of the processing is likely to make the process of compliance with the legal duties stemming from the data protection framework full of uncertainties and difficulties.

The document, therefore, can be seen as an **instrument to facilitate the final evaluation** of the techniques used in the processing and to enhance compliance with the DPIA obligations and, more in general, with the principle of accountability.

Due to the fact that it is a useful tool to guide the data controller on the road of compliance, we strongly promote its usage, not only in the particular context of SUCCESS, but also in the more general environment of smart grid systems.

4.8 Service recipients' rights and freedoms

Now is the moment to provide **specific guidelines for the protection of users' rights**. Given the delicacy of the matter at hand, we would like to point out the fact that the protection of the

---

[44] In the 2012 Recommendation it is stated that «in order to mitigate the risks on personal data and security, Member States, in collaboration with industry, the Commission and other stakeholders, should support the determination of best available techniques for each common minimum functional requirement listed in point 42 of the Recommendation».

[45] Smart-Grid Task Force Stakeholder Forum, Identification and Selection of Best Available Techniques for the 10 common minimum functional requirements related to the Smart Metering System roll-out under a Cyber-Security and Privacy Perspective - Best Available Techniques Analysis and Evaluation, 19/09/2016. https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp2_techniques_mapping_and_clustering.pdf

[46] Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (COM 2012/148/EU)

users' rights passes through two different paths. On the one hand, the controller is in charge of the **prevention of eventual infringements** of users rights. On the other hand, instead, the full enjoyment of their rights depends on the effective possibility to see **those rights enforced** by a public authority.

As already suggested in the context of this project, we recommend for all the operators of the energy distribution sector (in particular, for data controller, DSO and energy supplier) to set up all the organisational and technical measures in order to guarantee:

- **The right to access** smart meter data related to an individual user. This is a necessary step for compliance with the principle of transparency. It is probably implemented by providing the service recipient with an individual user interface for the purpose;
- **The right to erasure** of smart meter data of a person who is not a user anymore. In this sense, the data controller should ensure the possibility to remove from the system the personal data of the single user without damaging the integrity of the other data necessary for the functioning of the system. This can be achieved, for example, through the anonymisation of data.
- **The right to data portability.** The data controller should implement a system that, without lowering the security of data content, provides to users (at their request) all the data concerning them in an interoperable format.

5. Potential future work

Concerning the potential future work to carry out in this context, we suggest to focus the attention on the analysis of new technologies, giving particular attention to the new challenges that they may pose to the rights and freedoms of data subjects. Furthermore, the development of new technologies will also require the elaboration of innovative methods to carry out a DPIA in this field. Also, the possibility to involve data subject in the design of the privacy measures protecting them (e.g. through sample surveys) can be an interesting and viable path to enhance their privacy and provide them with an appropriate degree of control over their personal data.

6. Conclusion: how to develop a new era for data privacy in real time energy services

In this Deliverable we have tried to give a general overview of the influence that privacy and data protection law may have on smart grids. In particular, the whole project was based on identifying and solving cyber-threats (and privacy-issues) in the context of smart grids. Accordingly, this deliverable tries to summarize the methods elaborated both to protect the privacy of the end-user and to ensure the security of the "metering data" that are necessary for the functionality of the smart grid.

The structure of this deliverable has been as follows:

1. At first, we gave a **general look** at data protection law, highlighting its essential notions and their role in the data protection framework;
2. Secondly, we exposed the **specific solutions** that have been designed in the SUCCESS context;
3. Finally, starting from specific SUCCESS solutions, we tried to **extrapolate some principles that can be considered generally valid** in the energy and smart grid context.

The results of this project, in fact, far from being something that can be fruitfully used only in SUCCESS' context, are **rich of solutions that can be implemented in other contexts** to solve the problems created by the development of new energy systems.

In conclusion, reconciling **cyber security and privacy** can be a hard challenge within the energy sector. The SUCCESS project has for sure contributed to solving the challenges posed by this new situation. Moreover, the project has studied and elaborated a comprehensive set of guidelines and best practices that can be used in all the situations where there is the urge to protect the personal data of the end-users of smart grids without obstructing the processing activities.

7. References

Article 29 Working Party, Guidelines on the right to data portability, WP 242, Brussels, 13 December 2016

Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 2017, Brussels, April 2014

Article 29 Working Party, Opinion 12/2011 on smart metering, WP 183, Brussels, April 2011

CNIL, Methodology for Privacy Risk Management: How to Implement the Data Protection Act. 2012 Edition, 2014. Available at http://www.cnil.fr/english/publications/guidelines

Eskens, Sarah, "Profiling the European consumer in the Internet of Things: how will the general data protection regulation apply to this form of personal data processing, and how should it?", 2016, p. 19. Available from: https://ssrn.com/abstract=2752010. Accessed: 5 April 2018.

European Commission Recommendation on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, 2014/724/EU, 10 October 2014

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*, Brussels, 2014.

Farac, Robert et al., Description of Available Components for SW Functions, Infrastructure and Related Documentation, V1, Deliverable 4.4, SUCCESS - Securing Critical Infrastructure, Forthcoming 2017

Fiorentino, Giampaolo; Mantovani, Eugenio; *Privacy-Preserving Information Security Architecture V1*, Deliverable 3.1, SUCCESS - Securing Critical Infrastructure, July 2016.

Malgieri Gianclaudio, Mantovani, Eugenio; De Hert Paul; Corsi Antonello, Fiorentino Giampaolo, *Privacy-Preserving Information Security Architecture V2*, Deliverable 3.2, SUCCESS - Securing Critical Infrastructure, April 2017.

Gellert, Raphaël, "The Redefining the smart grids' smartness. Or why it is impossible to adequately address their risks to privacy and data protection if their environmental dimension is overlooked"; Journal of Law, Information and Science, Vol 24(1) 2016

Helberg, Natali, "Profiling and targeting consumers in the Internet of Things: a new challenge for consumer law", 2016. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717. Accessed: 5 April 2018

Kloza, Dariusz; van Dijk, Niels; De Hert, Paul, "Assessing the European approach to privacy and data protection in smart grids. Lessons for emerging technologies", in Florian Skopik; Paul Smith (ed.), *Smart Grid Security: Innovative Solutions for a Modernized Grid*, Elsevier, 2015. p. 11-47.

Malgieri, Gianclaudio; *Recommendation on How to Develop Data Privacy Compliant Countermeasures, Deliverable 2.1*, SUCCESS - Securing Critical Infrastructure , October 2016

Mantovani, Eugenio; Böröcz, István, <deliverable title>

Moerel Loekke, "GDPR conundrums: Processing special categories of data", IAPP, 2016, p. 44. Available from: https://iapp.org/news/a/gdpr-conundrums-processing-special- categories-of-data/. Accessed: 24 April 2018

Sanduleac, Mihai et al., Next Generation Smart Meter, Deliverable 3.7, SUCCESS - Securing Critical Infrastructure, Forthcoming 2017.

Sauba, Ganesh et al., Identification of existing threats V2, Deliverable 1.2, SUCCESS - Securing Critical Infrastructure, Forthcoming 2017.

Van der Sluijs, Jeroen et al., *Policy recommendations: Towards socially robust smart grids*, Utrecht, April 2015 – EPINET Deliverable D8.3.

May be add https://doi.org/10.1109/COMST.2017.2720195 and https://people.kth.se/~gyuri/Pub/DBGC-Power-HotCloud2013.pdf ?

7.1 Legislative references:

Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC Text with EEA relevance

E-privacy Directive, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

General Data Protection Regulation, 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 and on the free movement of such data, and repealing Directive 95/46/EC

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

8. List of Abbreviations

BMS	Building management system
BGW	Breakout Gateway
DSO	Delivery Service Operator
CI-SOC	Utility Security Monitoring Centre
DPIA	Data Protection Impact Assessment
DV	Double Virtualization
EAC	Exploitation Activities Coordinator
ERP	Enterprise Resource Planning
ESB	Electricity Supply Board
ESCO	Energy Service Companies
ESO	European Standardisation Organisations
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
GE	Generic Enabler
HEMS	Home Energy Management System
HV	High Voltage
I2ND	Interfaces to the Network and Devices
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
IoT	Internet of Things
KPI	Key Performance Indicator
LV	Low Voltage
M2M	Machine to Machine
MPLS	Multiprotocol Label Switching
MV	Medium Voltage
NIST	National Institute of Standards and Technology
NORM	Next Generation Open Real Time Smart Meter
O&M	Operations and maintenance
OPEX	OPerational EXpenditure
PM	Project Manager
PMT	Project Management Team
PMU	Phasor Measurement Units
PPP	Public Private Partnership
PUF	Physical Unclonable functions
QEG	Quality Evaluation Group
RBAC	Role Based Access Control
S3C	Service Capacity; Capability; Connectivity
SAU	Substation Automation Unit

SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SDN	Software defined Networks
SDOs	Standards Development Organisations
SET	Strategic Energy Technology
SET	Strategic Energy Technology
SG-CG	Smart Grid Coordination Group
SGSG	Smart Grid Stakeholders Group
SME	Small & Medium Enterprise
SMG	Smart Meter Gateway
SMS	Security Monitoring Solutions
SoA	State of the Art
SON	Self Organizing Network
SS	Secondary Substation
TL	Task Leader
TM	Technical Manager
USM	Unbundled Smart Meter
VPP	Virtual Power Plant
WP	Work Package
WPL	Work Package Leader