SUCCESS

D4.10 v1.0

Innovative approach to data privacy for 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:	30.04.2018
Actual Delivery Date:	30.04.2018
Contributors:	VUB
Workpackage:	WP4 – Securing Smart Infrastructures
Security:	PU
Nature:	R
Version:	1.0
Total number of pages:	34

Abstract:

This deliverable elaborates on an innovative approach to data privacy for energy services. It 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 energy services.

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.

Keyword list:

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

Executive Summary

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 energy services.

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.

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

1. finding related *privacy principles* in the primary and secondary EU legislation (Section 2);
2. translating such principles into *privacy guidelines* for the energy sector (Section 3);
3. translating those *guidelines* into *best practices*, according to the recommendations used in SUCCESS project (Section 4);
4. translating those best practices into technical privacy-by-design solutions developed within SUCCESS project (Section 4).

Authors

Partner	Name	e-mail
Vrije Universiteit Brussel		
	Gianclaudio Malgieri	gianclaudio.malgieri@vub.ac.be

Table of Contents

1. Introduction

1.1 The challenge of privacy protection within the provision of Energy Service

Generating "intelligence" in the power grid, for example, for implementing efficient energy distribution, flexible load management and dynamic pricing, requires the collection and analysis of huge amounts of data. Some of the data are private, e.g., those frequently measured by smart meters, and must not be leaked to untrusted or to third parties. Motivated by these privacy issues, various smart grid services have started integrating privacy-preserving schemes into their design and implementation, e.g., for billing, for voltage control etc., but a scalable solution that serves several services simultaneously, and at the same time ensures non-repudiation and allows for auditability does not yet exist.[1]

The SUCCESS project positions itself in this context. Its principal aim is "designing, developing and validating a novel holistic adaptable security framework which is able to significantly reduce risks of cyber threats and attacks" (DoW, p.10). SUCCESS is therefore a system whose purpose is to guarantee the safety of smart grids. As any smart grid application, albeit a particular one, i.e., one developed for guaranteeing the security of the network, the SUCCESS security solution requires to process personal data, in order to work and, for instance, to detect anomalies in the flow of consumption data. As such, it must also respect the legal requirements for data communication, which include respect for the personal data and the privacy of consumers.

1.2 The relevant legal framework

In response to the concerns that smart grid technology creates, the legal frameworks on privacy and data protection are often evoked as limits and safeguards. Privacy and personal data protection do not exhaust all societal concerns on smart grids, though they constitute one of the main issues at stake.[2] However, they constitute the main issue at stake in the context of SUCCESS.

In particular, we mention Article 8 of the European Convention on Human Rights (right to private and family life); but also Article 7 of the European Union Charter of Fundamental Rights (right to private and family life) as well as Article 8 of the same Charter (right to protection of personal data). We must refer also to secondary law, in particular to the General Data Protection Regulation (Reg. EU 2016/679), but also to the e-privacy directive (Directive 2002/58/EC). We must take into account also other relevant legal frameworks, i.e. the NIS Directive (Directive EU 2016/1148) concerning measures for a high common level of security of network and information systems across the Union and the Council Directive on European Critical Infrastructures (Directive 2008/114/EC).

Accordingly, energy service providers need to design a privacy friendly technology tool so that, e.g., it can only record activity at certain times of the day, or destroy data in a predefined time lapse.

1.3 Guidelines, Best Practices and Privacy-by-design approach

Taking the example of the SUCCESS Solutions, we can infer important guidelines and best practices for a new (privacy-enhancing) era in the provision of energy services and translate them into technical privacy-by-design solutions.

Indeed, the SUCCESS project has aimed also at designing and implementing a privacy-preserving solution for smart metering by combining state-of-the art and novel techniques into a single approach.

In particular, in the objectives of the Project there were key elements: Metering Data Protection; Anonymization of Metering Data and Privacy-Preserving Data Aggregation[3].

---

[1] See Asghar et al "Smart meter data privacy: a survey"IEEE Comunications Surveys and Tutorials, Nov. 2017 (https://doi.org/10.1109/COMST.2017.2720195).

[2] ibid p.19.

[3] See SUCCESS Deliverable 2.1 for more details on that.

In more specific terms, all Energy services could take these best practices for a new generation of privacy management in the Energy Sector:

- **Metering Data Protection**, which consists in the development of research on the most secure encryption/computing scheme which will address customers' concern that their personal information (e.g. their living habits) might be exposed to other parties from frequently collected metering data. The research will also examine how to anonymize the fine-grained meter readings without negatively affecting network operations, billing applications and potential third party services.
- **Anonymization of Metering Data**, which consists in the exploration of opportunities for separating the measurement data (meter readings) from customer IDs. Through separation, the overall meter readings or even the detailed energy consumption cannot be linked to individuals.
- **Privacy-Preserving Data Aggregation**, which consists of the investigation about the feasibility to enact actions such as online aggregation of data from geographically co-located consumers so that utilities have access to the aggregated metering information only, rather than to that of a single household.[4]
- **Anticipated and continuous Data Protection Impact Assessment (DPIA):** the first step consists in delivering recommendations for designers and stakeholders involved in the Architecture design;[5] the second step consists in an intermediate Data Protection Impact Assessment that takes into account the state of the architecture design before that it is completed;[6] the third step consists in the final Data Protection Impact Assessment after that the technology has been implemented.[7]

These objectives are particularly relevant for the so-called "privacy-by-design" approach.

Indeed, the EU's data protection approach applies anytime personal data is being processed. In essence, data protection is a set of principles, procedures and safeguards designed to ensure the transparency of data processing, so that individuals are able to know what happens to data concerning them. The notion of personal data is defined in art. 4 (1) of the newly introduced General Data Protection Regulation as *"any information relating to an identified or identifiable natural person".*[8] SUCCESS Solution will very likely process personal data. The principles, procedures and safeguards with the development of the SUCCESS prototype include *inter alia*:

- The need to process data in a manner consistent with good processing principles including:
  - Data minimisation and purpose limitation
  - Fairness, lawfulness and transparency of processing
  - Sensitivity and confidentiality of data
  - The right to review and correct data
  - Other principles, such as: data security, anonymisation, encryption, data protection by design and by default, impact assessment (IA), etc.)
- The need for a correct legal basis for the processing of data, such as consent
- The potential need to notify national data protection authorities about the main details of processing personal data.

[4] See DoW, p. 23.

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

[6] See SUCCESS Deliverable 3.2.

[7] See SUCCESS Deliverable 3.3.

[8] 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 (General Data Protection Regulation) (hereinafter GDPR in footnote and GDPR or "the Regulation" in the text)

An important data protection tool that has been developed purposefully to tackle the concern of the public towards smart grids is the data protection impact assessment. The need to conduct an impact assessment was already underlined by the European Commission in its Recommendation on the preparation for the roll out of smart metering systems of 9 March 2012, mentioned earlier.

In the spirit of the accountability principle that permeates it, the 2016, newly adopted, general data protection regulation introduces a requirement to obligatorily conduct a data protection impact assessment for specific processing operations (art.35). According to the 2012 recommendation, “the data protection impact assessment should describe the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC, taking into account the rights and legitimate interests of data subjects and persons concerned.”

1.4 The structure of this deliverable

Since we argue that it is important to offer a general overview of the relevant **European primary legislation** and in particular on the rules from **secondary legislation** in order to make recommendations for data privacy compliant countermeasures, Section 2 illustrates the notions of privacy and data protection from a legal point of view, listing the main legal references, and explaining the main principles and rules and their relevance for SUCCESS.

Section 3 addresses more specifically selected countermeasures and the so called “trade-off privacy/security”, according to Article 29 Working Party and U.S. NIST recommendations.

Finally Section 4 summarizes how the **privacy-by-design measures developed in SUCCESS could be exported, implemented and re-used as best practices for a new generation of privacy-friendly energy services.**

2. Applying the Data Protection Framework to smart energy services. Issues and opportunities

2.1 The Fundamental Rights to Privacy, Data Protection and Smart Meters

As mentioned earlier, smart meter data can offer **sharp insights into consumers' energy use** and consequently **into their end-users' private habits at home.**

In this context, the European Commission, established in 2009 the **"Smart Grids Task Force",** consisting of four experts groups and one of them was charged with providing **regulatory recommendations for privacy, data protection and cyber-security in smart grids and metering environments[9].** Based on the work of this Task Force, in **2012** the **European Commission issued a non – binding Recommendation on the roll out of smart grid and smart metering systems[10]**.

The 2012 Recommendation addresses three main aspects: 1) **personal data protection,** 2) cost-benefit analysis, and 3) **common minimum functional requirements of smart meters**.

With regard to the first aspect, it clearly states that "*the 1995 Data Protection Directive applies and clarifies its application to the nature and needs of smart grids"*. It further advises on six "tools" for achieving an adequate level of personal data protection: **1) data protection by default and by design**, **2) privacy certification, Privacy Enhancing Technologies (PETs)**, in particular **anonymisation** and **encryption**; and **3) Best Available Techniques (BATs).** However, one of the most important legal tools in order to implement privacy of users in concrete is **4) Data Protection Impact Assessment (DPIA).**

The 2012 Recommendation provides for a comprehensive action-framework **to tackle privacy and data-protection aspects in smart grids and smart metering environments**. The Recommendation has been supplemented by a series of **opinions**, **guidelines** and **studies by relevant bodies** within or interacting with **the European Commission**.

Further to this, the **2012 Energy Efficiency Directive has introduced a specific provision in its article 9.2.b that stipulates** that**:** *"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".***

Subsequently another process was launched, concerning the elaboration of an *ad hoc* template for the development of **Data Protection Impact Assessments** when **intelligent metering systems are deployed.** The first phase of the process was concluded through 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)[11].

All these documents supplement (and do not replace) the existing, legally binding personal data protection framework thus creating a complex multi-layer approach towards personal data protection aspects in the context of smart meters which may result difficult to use in practice[12].

---

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

[10] 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).

[11] 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.

[12] 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.

2.1.1 Personal Data in Smart Metering Environments and SUCCESS

In addition to the definition of personal data in EU Data Protection Legislation[13], some **energy sector-specific definitions exist**.

In order to help market actors to interpret Data Protection rules when applied to smart grids and metering environments, the European Commission has set-up an expert group called *the Smart Grid Task Force*.

The Task Force has provided for a non-exhaustive list of what is to be considered as "personal data" in the context of smart metering systems[14]:

- Household's consumption:
- Consumer registration data: names and addresses of data subjects, etc;
- Usage data (energy consumption, demand information and time stamps), as these provide insight in 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 in 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 in the daily life of the data-subject;
- Billing data and consumer's payment method

The Task Force also provides for a set of illustrative examples. The following seem to apply to the SUCCESS context.

2.2 Relevant Requirements from EU Data Protection Law for the development of SUCCESS countermeasures

Below is a list of requirements from data protection law **identified as important for any security countermeasure that SUCCESS project will develop.** This list is not claimed to be the complete list of requirements against which the **project research** and **technology** will have to be assessed. It elaborates on **elements that emerged as relevant until the moment of finalising this report**, such as the different roles and responsibilities among entities in data processing; the secondary use of data collected vs. the purpose limitation principle; legal implications of data pseudonymization and Data Protection Authorities competent for any processing led either during SUCCESS project or after the implementation of the project.

2.2.1 An important disclaimer: the protection of "personal data" of legal persons in the SUCCESS project

An important disclaimer is needed: **the protection of data privacy applies only in cases where final customers (or their data) are involved**.

[13] Art.4 (1) of the 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".

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

When there is no individuals' involvement, the EU data protection legal framework cannot apply. Indeed, article 1(1) of GDPR affirms that the scope of the protection afforded by this Regulation should apply only to *natural persons*, in relation to the processing of their personal data. Furthermore, recital 14 of the GDPR clearly states that "the protection afforded by this Regulation should apply to *natural persons*, (…), in relation to the processing of their personal data. 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 personal data protection of legal persons and specifically **for the protection of legal persons' information which are "sensitive" in terms of competition policies**, the EU legal framework offers a different tool: the **protection of trade secrets**[15], which is now regulated explicitly at the EU level by a new directive: the Directive (EU) 2016/943[16].

However, 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.

Actually, if data of legal persons include personal data of legal persons' customers or in general include personal data of individuals, the GDPR applies. What is necessary in such cases is to determine different roles and responsibilities in the data protection framework.

In other words, in such cases the two legal persons might be either joint-controllers (if they jointly determine scope and means of the processing of data of customers) or play different roles.

2.3 Data protection principles (applicable to SUCCESS Solutions)

2.3.1 The principle of fair, lawful and transparent processing

Data subjects should be able to know what information has been collected about them, the purpose of its use, and who can access and use it. Users should also be informed about: how to gain access to information collected about them and how they may control who has access to it. To achieve this, the transparency of the data processing should be ensured.

Data controllers (see description below) should be **clearly identified** and be **able to respond to requests** of e.g. data subjects.

2.3.2 The principles of data minimisation and purpose limitation

According to the **data minimisation principle**, information systems and software shall be configured by **minimising the processing of personal data**. The "purpose limitation" principle[17] **prohibits further processing** which is **incompatible** with **the original purpose(s) of the collection.**

2.3.3 The principle of data quality

The principle of **data quality** ensures that data are "adequate", relevant and not excessive in relation to the purposes for which they are collected and / or further processed, as well as accurate and, where necessary, kept up to date.

2.3.4 Legitimate grounds for processing

The choice of the **legal basis** for these **processing operations** has to be carefully **selected** and duly **justified**. The article 7 of Directive 95/46/EC and article 6.1 of GDPR offer a series of **possible legal bases** that might be applied.

[15] 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.

[16] 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).

[17] Art. 6 (1) b) of Directive 95/46/EC

Further guidance on the processing of Smart Metering data and compliance with the Data Protection Directive can be found in the Article 29 Working Party opinion WP183 on smart metering.

2.3.4.1 Special Categories of Data: Sensitive Data

Sensitive data is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and concerning health and sexual orientation[18]. The EU legal regime towards this type of data is prohibitive and can only be waived out under specific circumstances such as, for instance: the data-subject has given explicit consent to the processing of those personal data for one or more specified purposes[19], and other conditions listed in article 9.2 from indent (a) to (j) of the GDPR.

Even though this prohibition **may not seem relevant** in the context of **smart meter data**, and especially **data that needs to be processed** by the **SUCCESS partners**, examples can be given where these data do provide an insight into, for instance, **religious beliefs,** as **energy consumption can reveal patterns of, for example, observing Ramadan or getting ready for morning prayers[20].**

2.4 Fundamental Notions

2.4.1 Consent

For the act of processing to be **"lawful",** personal data should be processed on the basis of the **consent of the data subject concerned**[21].

Consent is described as an act expressing unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. The Regulation mentions typical forms of consent, including for instance, a written statement, including by electronic means. Consent is described according to several specific cumulative attributes[22].

It **must** be:

- clear;
- affirmative;
- freely given;
- specific and
- informed

The expression of consent could include ticking a box when visiting an internet website, choosing certain technical settings when using online services or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data[23].

Consent should cover **all processing activities** carried out for a **specific and defined purpose.** When the processing has **multiple purposes**, consent **should be given for all of**

[18] Article 9.1 of GDPR and

[19] 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).

[20] 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) .

[21] For the processing to be lawful, personal data can be processed also based on other legitimate basis, laid down by law, or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Consent does not provide a valid legal ground for the processing in the case there is a clear "imbalance" between the data subject and the controller.

[22] Article 4 (11) of GDPR.

[23] Recital 32 of GDPR.

them[24]. Consent should **not** be regarded as **freely given** if the data subject has **no genuine or free choice** or is unable **to refuse or withdraw** consent **without detriment**[25].

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

2.4.2 Special Categories of Data Subjects

Children are considered as vulnerable natural persons under GDPR (Recital 75) and enjoy specific protection with regard to their personal data. They are regarded as data subject for data protection law.

It may be possible, depending on level of accuracy and frequency of the readings **to identify personal data related to children or people affected by sickness out of smart meters' data.** By analysing detailed electricity usage data it may be possible to predict – also on a basis of deductions about the way in which electronic tools work - when members of a household are away on holidays or at work, when they sleep and awake, whether they watch television or use certain tolls or devices, or entertain guests in their free-time, how often they do their laundry, if someone uses a specific medical device or a baby-monitor, whether a kidney problem has suddenly appeared or developed over time[26], if anyone suffers from insomnia, or indeed whether individuals sleep in the same room[27].

The SUCCESS consortium will have to carefully analyse the features of the meters that the secure smart grid infrastructure will make use of to gather the measurements. The project should avoid "unnecessary" data processing and the transmission of very frequent and very detailed data.

This means avoiding any unnecessary collection and use of personal data (data minimisation principle), and limiting the transfer and any processing of the data solely to the specific purpose of the Project (principle of purpose specification). For **data remaining "necessary"**, **legal safeguards "by design"** and **"by default"** should apply. As **provisions in this area are technical**, the project may need to **involve data protection Authority** also in line with the **European Commission recommendations issued in 2009 and 2012 on smart metering environments.**

2.4.3 Processing

Processing means any operation which is performed on personal data (or on sets of personal data), whether or not by automated means, such as 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 (Article 4.2 of GDPR)[28].

As a general rule, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means (*Recital 39* of GDPR).

Any processing of personal data should be (cumulatively):

[24] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance. Recital 43 of GDPR.

[25] Recital 42 of GDPR.

[26] In case of processing special categories of data, such as data related to one's health, consent must be explicit and supported by evidence that its processing is necessary to attain a legitimate goal. Art. 8 (1) of the 1995 Directive. In order to process medical data, it is necessary to inform the doctor who has a therapeutic link to the patient.

[27] Mireille Hildebrandt, 'Legal Protection by Design in the Smart Grid. Privacy, Data Protection & Profile Transparency' 88.

[28] 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.

- lawful,
- fair and
- transparent

towards data-subjects on:

- the personal data which is collected from them;
- on how it is used and
- to what extent it is used.

The personal data collected should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. In order to ensure that the personal data are not kept longer than necessary, time limits must be established by the controller for erasure or for a periodic review. Further to this, every reasonable step should be taken to ensure that personal data that are inaccurate are rectified or deleted[29].

Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access and the equipment used for the processing[30].

Whenever processing personal data, SUCCESS's partners should consider if it is absolutely necessary for operational purposes; if the processing is not "absolutely necessary", it should be avoided whenever possible[31].

As mentioned earlier, given the delicacy of this matter it is strongly recommended that in the context of SUCCESS, the purposes and contents of the processing are identified to the largest extent possible before the consent of the end-users is sought so to reduce the risks linked to the controller's accountability over processing activities established by law.

2.4.3.1 Processing activities in smart metering environments

The non-exhaustive list below provides some illustrative examples of **processing of personal data in smart meter environments**[32]:

- 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 naming addressing, encryption, data plausibility mechanism (e.g. detecting tampered data);

In the case of "**prosumers**", the operation of **preparing aggregated data necessary for energy efficient maintenance of the grid** (forecasting and settlement) does **not request user consent** and may be considered as a legal obligation of the smart grid operator[33].

This matters for SUCCESS's prosumers as the project may need to enter in dialogue with the local DSOs to clarify and determine what the (secure) smart grid service will do additionally or differently to / from the DSOs tasks.

[29] Recital 39 of GDPR.

[30] Recital 39 of GDPR.

[31] Smart Grid Task Force 2012, 14 Expert Group 2, Regulatory Recommendations for Privacy , Data Protection and Cyber-Security in the Smart Grid Environment Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, p.14.

[32] ibid p. 19.

[33] Article 29 WP Opinion WP205.

2.5 A special remark for secondary uses, purpose limitation and consent in smart grids security systems

A problem that smart grid security systems may have concerns the purpose limitation principle and so the necessity of a specific consent for any specific processing of data.

Indeed, smart-grid-security systems, like the one potentially developed by SUCCESS, may need to process personal data for purposes other than that for which the personal data have been collected with data subject's consent.

This is due to possible new threats detected after the contract with the customer, or new and innovative security techniques developed after the collection of data.

Recital (50) affirms that the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed **only where the processing is compatible with the purposes for which the personal data were initially collected.** In such a case, no legal basis separate from that which allowed the collection of the personal data is required.

This is particularly useful for the needs of entities that are involved in the provision of smart grids services, because it is undoubted that asking anytime new consents to customers is somehow ineffective in terms of security, survivability and resilience.

In particular, article 6(4) of GDPR clarifies that in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, the controller "shall take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding **the relationship between data subjects and the controller**;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymization".

Some of these points are particularly relevant for SUCCESS project: pseudonymization can be easily achieved for the most of processing also for cyber-security reasons. Moreover, "the link between purposes" and "the relationship between data subjects and the controller" can be easy elements that help to ascertain that the new purpose is compatible with the initial purpose for which data have been collected and as such no new consent must be asked to customers.

A specific recommendation that we propose is to increase pseudonymization to the whole data processing or at least as much as possible.

A final remark must be dedicated to "further processing" for the development of SUCCESS project. Indeed, recital (50) clarifies that "further processing for archiving **purposes in the public interest, scientific** or historical **research purposes** or statistical purposes should be considered to be compatible lawful processing operations".

2.5.1 Controller, processor and sub-contractors in smart grids: a golden rule for the allocation of responsibilities

Another relevant issue is to understand who plays the role of controllers and processors in the complex framework of smart grids, even when considering the various sub-contractors.

The golden rule is that <u>when an entity determines scope and means</u> of data processing will be considered <u>data controller</u>, with all duties and responsibilities described above, and anyone acting according to its instructions and control is a data processor.

As soon as it loses the control on scope and means of data processing and a new subject acquires such control, the first is not a data controller any longer and the new subject becomes the data controller.

Instead, if the first subject does not lose the control on scope and means but it just shares it with another subject, the two entities become “joint controllers”.

As such, they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of GDPR, by means of an arrangement between them”

We will make now some specific examples.

In some Member States, the legal person with the most responsibility for processing personal data would be the **energy supplier**. They have the contract with the final customer which initiates the processing and by deciding which data they require to fulfil their functions and how they will collect, store and use the data, they can obviously be said to have determined the purposes for which, and the manner in which, the personal data are processed. This establishes them quite clearly as a data controller for the processing of personal data generated by an energy meter[34]

In other models, the **DSO** which owns the smart grid will be responsible for the installation and running of the Smart Meter system. Since the DSO will also be responsible for determining how the data are collected, stored and used, it will be a data controller. Where the energy suppliers have the right to access the data transmitted by the meters and are using the data for their own purposes (for example, to issue bills or to give advice to consumers) then they will also be a data controller for the personal data they are processing.[35] It could be a case of joint controllers.

Moreover, in some implementation models where a central communications function is established which has responsibility for managing the transmission of data between the meter and the supplier, it will be the data processor if it acts only on the instructions of the suppliers to and from whom it sends and receives data. Instead, if in any case the communications function is engaged in deciding whether personal data can be disclosed to a third party, or whether such data can be processed for new purposes, then the communications function **could assume the role of data controller** in respect of that personal data processing.[36]

However, third party service providers, for example **Cloud service providers for smart data back up in the development of the SUCCESS project**, will have an increasingly prominent role in the use of data generated by smart meters. Where personal data are disclosed to the such third parties in order for them to provide a service either to the consumer or to another party, such as a supplier, then **the third party will assume the role of a data controller**. [37]

This is an increasing reality in the SUCCESS project. Indeed, one objective of SUCCESS is implementing a “scalable cloud-based mixed software/hardware stack enriched with security features placed on the top of NOBELGRID meter”.

The cloud provider, as a third-party service provider, plays therefore a crucial role. It is a data processor, but for some data processing he will determine scopes and means and so he will be (at least a joint) data controller.

2.6 Data Protection Impact Assessment

Art. 35 of GDPR requires the data controller to conduct an assessment of the impact of the envisaged processing operations on the protection of personal data, when a type of processing is likely to result in a high risk for the rights and freedoms of the individual.

[34] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering (4 April 2011), 9.

[35] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering (4 April 2011), 9.

[36] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering (4 April 2011), 10.

[37] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering (4 April 2011), 11.

The data protection impact assessment is intended to implement the general risk assessment logic into data protection law. With such assessment the controller is capable to determine whether the risk (the processing of personal data) has negative consequences and if so, how to treat them (by implementing mitigation adequate measures).

In any case, prior consultation of the supervisory authority may be required in the case the assessment reveals that the processing of personal data would result in a high risk in the absence of measures taken by the controller to mitigate such risk[38].

2.6.1 DPIA and BAT (Best Available Technologies) in Smart Metering Systems

In order to conduct a correct risk assessment, the data controller should consider existing threats, security issues and possible solutions.

Actually, **it is evident that stakeholders have differing perspectives on and approaches to security**, probably reflecting different perceptions of likely threats, but also corresponding to the various architectures involved in Member State deployments. There are also differences in the perception of privacy, which most probably can strongly influence the data protection impact assessment framework.

For this reason, the *Smart-Grid Task Force* launched in October 2014 an initiative aiming at conducting a first Best Available Technique assessment process relying on the contributions of an ad-hoc created Stakeholder Forum (SF).

Such document[39], through the application of the evaluation framework adopted by the stakeholder forum in 2015, focuses specifically on **the evaluation of the techniques, gathered during the BAT** data collection phase ended in spring 2016, used today to ensure privacy and cyber-security in smart-metering systems with respect to the 10 minimum functional requirements described in the Recommendation 2012/148/EU1 and in alignment with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

The document must be intended as an instrument to facilitate the final evaluation of the techniques and so to correctly comply with the DPIA obligations. In other terms, it is *a good tool that SUCCESS partners can use in order to comply more easily with data privacy obligations*.

2.7 Transferring data outside the EU[40]

For **transfers outside the EU**, more stringent rules apply. The logic behind this is that countries outside the Union **may not have the same level of data protection in their law** as the countries of the Union (where GDPR applies).

There is no need to transfer personal data outside the EU in SUCCESS. However, the project may need to use 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 due consideration.

Art. 45 GDPR requires a **third country to ensure an adequate level of protection** that is evaluated by the Commission. If the Commission has decided that the country in question has **no adequate level** of protection, **a controller** or processor **may transfer personal data to a third country only if** the controller or processor **has provided appropriate safeguards[41],** and

[38] Art 36 of GDPR

[39] 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.

[40] This chapter was written after 23 June, therefore the results of the referendum about the United Kingdom leaving the European Union should be taken into consideration. Although it is too early to predict the consequences of the referendum, the possibility of the UK becoming a third country in terms of data protection law.

[41] These safeguards can be inter alia

(a) a legally binding and enforceable instrument between public authorities or bodies;

on condition that enforceable **data subject rights** and **effective legal remedies for data subjects** are available. When **neither the country provides adequate safeguards**, **nor the controller ensures the required safeguards,** personal data can be transferred to third countries only if additional conditions[42] are met.

The most important (in the case of the SUCCESS project) of these conditions is where the data subject gives his **explicit consent to the proposed transfer.** In order to utilise this option, it is necessary to explain to all data subjects involved that their personal data will be transferred to a state outside the EEA and that such transfer is **to an area where EU rules on data protection do not apply.**

Each controller has a counter-part in a Competent Supervisory Authority.

The competent supervisory authority should be the supervisory authority of the Member State where the controller has its main establishment.

However, as for the Data Protection Authority to whom end-users can appeal, EU Data Protection Legislation attributes this responsibility to the **National Authority based in the Country where the data is processed.** However, **SUCCESS end-users** should be enabled to **recur to their own national DPAs** not least for a question of **working "language".** This **aspect is very important for the project to ensure data-subjects enjoy their rights.**

In Countries where DSO has exclusive controllership rights on readings, do DSOs also hold exclusive rights on readings of sub-metering systems?

There is a "grey area" in this respect. EU legislation on "smart metering" does not always explicitly refer to "smart meters" only.

EU Legislation applies to **"smart metering system"** or **"intelligent metering system"** that are **"generally" defined as**: "an electronic system that can measure energy consumption, providing

---

(b) binding corporate rules in accordance with art. 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

[42] As to article 49, these conditions 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;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

more information than a conventional meter, and can transmit and receive data using a form of electronic communication" (article 2 point 28 on Definition of the 2012 Energy Efficiency Directive[43]). **The SUCCESS consortium thus needs to further inquire on this aspect as this definition may apply to sub-meters as well.**

This may not apply to Belgium since provisions on intelligent metering - in particular art 9.2 on "metering" and 10.2 on "billing" of the Energy Efficiency Directive - are applicable where and to the extent that Member States implement intelligent metering systems and roll out smart meters in accordance with the deployment stipulated by Annex I of the EU Electricity Directive 2009/72/EC.

[43] Directive 2012/27/EU of 25 October 2012 on energy efficiency,

3. Guidelines for an innovative data privacy era in the Energy Services

3.1 Two examples of guidelines: the EU approach and the US approach

We will consider in particular two lists of privacy guidelines for smart meters elaborated by two of the most relevant non-binding guidelines[44]: the EU Article 29 Working Party Opinion on Smart Meter and the guidelines for smart grids cyber-security from the U.S. National Institute of Standards and Technology (N.I.S.T.). We retake this comparison from our previous Deliverable 2.1 ('Recommendation on How to Develop Data Privacy Compliant Countermeasures').

A summary of data protection recommendations that could be useful for our purposes is offered by Article 29 Working Party (Art.29 WP/183) [45]:

- The prevention of unauthorised disclosures of personal data;
- The maintenance of data integrity to ensure against unauthorised modification;
- The effective authentication of the identity of any recipient of personal data;
- The avoidance of important services being disrupted due to attacks on the security of personal data;
- The facility to conduct proper audits of personal data stored on or transmitted from a meter;
- Appropriate access controls and retention periods;
- The aggregation of data whenever individual level data is not required.

Other interesting recommendations are formulated by the U.S. National Institute of Standards and Technology[46]**:**

- An organization should ensure that information security and privacy policies and practices exist and are documented and followed. Audit functions should be present to monitor all data accesses and modifications.
- Before collecting and sharing personal information and energy use data, a clearly-specified notice should be announced.
- Available choices should be presented to all users. Organizations need to obtain users' consent or implied consent if it is not feasible, with respect to the collection, use, and disclosure of their personal information.
- Only personal information that is required to fulfil the stated purpose should be collected from individuals. Treatment of the information should conform to these privacy principles.
- 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 be aggregated or anonymized wherever possible to limit the potential for computer matching of records. Personal information should only be kept as long as is necessary to fulfil the purposes for which it was collected.
- The organization should allow individuals to check their corresponding personal information and to request the correction of perceived inaccuracies. Personal information data subjects should be notified about parties with whom personal information has been shared.
- Personal information should be used only for the purposes for which it was collected.

[44] See G.Malgieri et al., SUCCESS Deliverable 2.1, Recommendation on How to Develop Data Privacy Compliant Countermeasures, 31 October 2016.

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

[46] 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.

Personal information should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the service recipient.
- Personal information in all forms should be protected from unauthorized modification, copying, disclosure, access, use, loss, or theft.
- Organizations should ensure the data usage information is complete, accurate, and relevant for the purposes identified in the notice.
- Privacy policies should be made available to service recipients. These service recipients should be given the ability and process to challenge an organization's compliance with their state privacy regulations and organizational privacy policies as well as their actual privacy practices.

Actually, the U.S NIST Recommendation is sometimes redundant in the EU framework: nearly all requirements are already mandatory by law in the European Union, as it appears evident from Section 2.

As we will see in Section 4, these best practices have been efficiently implemented in the SUCCESS Architecture and we will provide relevant details on that.

3.2 Guidelines on how to develop Data Privacy Compliant Countermeasures within the Provision of Energy Services

After this wide overview about data privacy legal rules applicable to smart grids security countermeasures and about the trade-off between privacy and security in designing smart grids security countermeasures, it is now necessary to *summarize all best practices useful in order to develop privacy compliant countermeasures*. In order to do so we ***rephrase, contextualize and update some of the "recommendations" already made in SUCCESS Deliverable 2.1 ("Recommendation on How to Develop Data Privacy Compliant Countermeasures").***

In the following paragraphs we will enlist all the recommendations in three different categories: the protection of access to data; the protection of data content; the protection of users' rights.

A preliminary group of recommendations concerns the definition of roles and responsibility. Indeed, determining who is the controller is necessary in order to understand to whom the recommendations are addressed.

3.2.1 Guidelines on the determination of "privacy roles" in smart grids security countermeasures

- As for the determination of the ***controller***, the **golden rule** is that when an entity determines scope and means of data processing it will be considered data controller, with all duties and responsibilities described above, and anyone acting according to its instructions and control is a data processor.
- When the determination of scopes and means is shared by two stakeholders they will be ***joint controllers***. As such, they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of GDPR, by means of an arrangement between them
- *Cloud service providers for smart data back-up* will have an increasingly **prominent role in the use of data generated by smart meters**. Where personal data are disclosed to such third party in *order for them to provide a service either to the consumer or to another party*, such as a supplier, then the third party will assume the role of a *data controller*.
- As for the role of final customers, they are ***data subjects***. However, final customers, as "prosumers", can be considered joint controllers, but only when their activity is not "purely personal": for example for customers who are landlord or who host guests in their houses for commercial activities (AirBnB, B&B, rental) or who use their property for professional activities.

3.2.2 Guidelines for the protection of *access to data*

It is a crucial field, because it combines both privacy concerns and security concerns. In other terms, as said before, the control of access to data can have a great impact both on the security of systems and on privacy itself.

In particular we recommend:

- **effective authentication** of the identity of any recipient of personal data;
- authorization of all accesses;
- prevention of **unauthorised disclosures** of personal data.

3.2.3 Guidelines for the protection of *content of data*

Protecting the quality of data content and of data processing in general is one of the most important challenges that a privacy by design approach should have regarding the development of smart grids security countermeasures.

In particular we recommend:

- **increasing the pseudonymization** to the whole data processing or at least as much as possible. In order to do that the controller must take technical and organisational measures necessary to ensure, that additional information for attributing the personal data to a specific data subject is kept separately.
- **avoiding any unnecessary collection and use of personal data** (data minimisation principle), and limiting the transfer and any processing of the data solely to the specific purpose of the Project (principle of purpose specification).
- aggregating data whenever individual level data is not required.

3.2.4 Guidelines for the protection of *user's rights*

Allowing users' to fully exercise their data protection rights is highly important in order to respect EU data protection law.

In particular we recommend:

- Continuous assessment of data processing purposes, lawfulness and fairness;
- available choices should be presented to all users. Organizations need to obtain users' consent or implied consent if it is not feasible, with respect to the collection, use, and disclosure of their personal information with precise description of scopes and means of the processing. A more detailed description of the consent form is provided for in Annex I, §1;
- a detailed notice about the specific purposes and means of data processing should be delivered to the user, it should include also all the possible future uses of data which can be predicted, *rebus sic stantibus*. A detailed description and exemplification of this notice is provided for in Annex I, § 2.

As for specific users' rights:

- right to access to smart meter data related to an individual user must be always guaranteed to such user. In order to do that, it would be necessary to allow users to access the platform with an individual interface, in order to respect recommendation made above (§ 4.2);
- right to erasure of smart meter data related to an individual user who is not a customer anymore must be always guaranteed. In order to do that, smart meter data related to a specific individual should always be removable from the platform without damaging the quality of other data processing and without renouncing to pseudonymization (§ 4.2 above);
- right to data portability must guarantee individual users the possibility to ask and receive all data related to them which they provided to the data controller (e.g. in a registration

form) in an interoperable format. This should be done without lowering the security of data content (including encryption and pseudo-anonymization) (§ 4.2 above).

We can thus summarize the best practices for the Energy sector as follows in Figure 1:

Data Protection Principles (Art. 5, GDPR)	**Privacy Guidelines for the Energy grids (§3)**
Data integrity	Data access controls (§3.2.2); Prevention of unauthorized disclosures (§3.2.2); Pseudonymization (§3.2.3)
Data minimization; Purpose limitation	Avoiding unnecessary use of personal data (§3.2.3)
Data storage limitation	Aggregating data as much as possible (§3.2.3)
Lawfulness, fairness, Accountability	Continuous assessment of data processing purposes and of the respect of users' rights (§3.2.4) Clear allocation of roles and responsibilities (§3.2.1)

Fig. 1: List of Privacy Guidelines in the energy sector compared with relevant Privacy Principles contained in the GDPR

As we can see, these guidelines are all related to a data protection principle as described in Section 2 (data integrity, data minimization, purpose limitation, data storage limitation, lawfulness, fairness, accountability).

4. Putting Privacy Energy Guidelines 'in practice': privacy-by-designs lessons from SUCCESS Project

Privacy Guidelines for the Energy Sector described in Section 3 need a practical implementation. That is why we will translate those guidelines in best practices. In particular, SUCCESS project proposes a list of best practices for developing privacy-enhancing solutions in the smart grids (already mentioned at the end of §1). Then, each of those best practices will find a relevant privacy-by-design solution in SUCCESS Architecture.

4.1 How Guidelines Summarized in Section 3 can be implemented in practice

A possible implementation of privacy guidelines for the energy sector (§3) can be found in the following list of best practices (as already mentioned in Section 1):

1. **Metering Data Protection**, i.e., performing research on the most secure encryption/computing scheme which will address customers' concern that their personal information (e.g. their living habits) might be exposed to other parties from frequently collected metering data.
2. **Anonymization of Metering Data**, i.e., separation of the measurement data (meter readings) from customer IDs.
3. **Privacy-Preserving Data Aggregation**, i.e., investigating about the feasibility to enact actions such as online aggregation of data from geographically co-located consumers so that utilities have access to the aggregated metering information only, rather than to that of a single household.[47]
4. **Anticipated and continuous DPIA,** i.e. recommendations for designers; intermediate DPIA and the final DPIA.

As it is shown in Fig. 3, each of these best practices can be perfectly related to one of the aforementioned privacy guideline principles for energy grids and with Data Protection principles contained in Article 5 of the GDPR.

Data Protection Principles (Art. 5, GDPR)	**Privacy Guidelines for the Energy grids** (§3)	**Best Practices for the Energy Sector** (SUCCESS guidelines)
Data integrity	Data access controls; Prevention of unauthorized disclosures; Pseudonymization.	Metering Data Protection
Data minimization; Purpose limitation	Avoiding unnecessary use of personal data	Anonymization of Metering Data
Data storage limitation	Aggregating data as much as possible	Privacy Preserving Data Aggregation
Lawfulness, fairness, Accountability	Continuous assessment of data processing purposes and of the respect of users' rights	Anticipated and continuous DPIA

Fig. 2. Practical Implementation (best practices) of Guidelines discussed in §3, with related Data Protection Principle in the GDPR.

[47] See DoW, p. 23.

4.2 The virtuous example of SUCCESS privacy-by-design solutions

SUCCESS Project has well implemented those best practices in technical solutions, that we can call “privacy-by-design” solutions, whose purpose was also to enhance the protection of personal data of end-users and energy operator physical persons.

In particular, the whole project was based on indentifying and solving Cyber-threats for smart grids and this can be for sure the best way to protect “metering data”, in accordance with Data Integrity principle.

In addition, the Smart Meter designed within SUCCESS (called “NORM”) collects personal data but does not share them with other components/agents/operators: there is an automated tool (called Role Based Access Control System) through which end-users can decide who (which kind of subjects based on their roles) can access their data, when, how and how long. In general, however, just network data (and not consumption data[48]) are shared, so there is no flow of personal data beyond the Utility level.

Another important solution is that access to data are controlled and logged, but since those logs are personal data (of the physical operator of the Energy Service) there is a system of anonymization: all data before leaving the Utility level.

In addition, in order to enhance security of data all information is stored in a Cloud (Smart meter Gateway), but this ‘virtualization of data’ (called ‘double virtualization’) is divided into two parts: there is a Data Layer and a Functionality Layer. Data Layer (where all personal data are stored) is totally separated from the Functionality Layer. This is a form of data minimization, though enhancing disaster recovery solutions.

Some of these privacy-by-design solutions will be discussed in an apposite sub-section below, in particular RBAC design, Double Virtualization and three step tests, while for cyber threat analysis we refer to the relevant deliverable of WP1.

Privacy Principles	Best Practices in theory in the Energy Sector	Best Practices in practice in the Energy Sector	Privacy-by-design solution in SUCCESS
Data integrity	Data access controls; Prevention of unauthorized disclosures; Pseudonymization.	Metering Data Protection	Cyber-threats analysis
Data minimization; Purpose limitation	Avoiding unnecessary use of personal data	Anonymization of Metering Data	NORM and RBAC System
Data storage limitation	Aggregating data as much as possible	Privacy Preserving Data Aggregation	‘Double Virtualization’
Lawfulness, fairness, Accountability	Continuous assessment of data processing purposes and of the respect of users’ rights	Anticipated and continuous DPIA	Three-steps test DPIA

Fig. 3: Comparison between Privacy Principles, best practices for the energy services and privacy-by-design solutions developed in SUCCESS

[48] We highlight that from network data it is not possible to infer consumption data.

4.2.1 NORM: RBAC and Privacy Profiles (PP)

The whole functioning of the Smart Meter developed in SUCCESS (which is called NORM) is based on a "database centric architecture"[49]. Any access of external actors qualified in SUCCESS Components **can be only done by accessing the central database of NORM through two specific interfaces, i.e. "MQTT"**, **which are incorporating role based access control (RBAC)**.

In particular, each end-user shall be asked to allow the DSO to access only specific data. In addition, the communication with the DSO and also with all others actors (e.g. ESCO or energy supplier) will be in a secure environment: the communication of data is made through the specific DSO's OpenVPN and the whole SCADA application is sandboxed in a Docker cluster containing an MQTT broker, the SCADA app with IEC61850 protocol and the OpenVPN client.

For these specific purposes, the NORM will be based on a "**User Privacy Profile" UPP** System that controls the whole system of accesses, and several accessory "**privacy profiles" (PP1, PP2, …, PPN**), **which are a combination of rights of data access for any specific qualified actors within the SUCCESS Components** (e.g. DSO is PP1, ESCO is PP2, etc.) and is based *both on a) specific National rules about smart grids maintenance and public security rules in the energy sector* (see in particular different national laws about DSO's data retention duties) and *on b) specific instructions given by the end-users through its UPP*.

The combination of a) national rules and b) user's instructions is fundamental also considering the EU Data Protection Law Framework.

In particular, the GDPR states at Article 6 that the processing of personal data can be based both on the consent of the data subject (or in compliance with a contract) or based on specific legitimate interests or national laws.

This double nature of PPs helps conciliate the two aspects of personal data processing principles *(users' controllership and national interests).*

Indeed, country specific rules are describing priorities between DSO and user preferences. For instance, for voltages the DSO may have the right to read the data, without consent of user, but for the active powers of the user consumption the user has the right to give or not this rich content and privacy sensitive data to any actor (including for DSO). The simplified scheme of PP construction is in the figure on the right side of the text.

The user platform, as already mentioned, is based on an Open Source / Open Access MQTT oriented platform called "SMXCore" available at this site: https://github.com/SMXCore/SMXCore_NG. By using SMXCore in NORM, each end-user (data subject) will be able to access his or her own specific user account on this platform where he or she can:

- access all personal data (users' data and active power, 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.).
- read purposes and any other meaningful information about the processing of data (according to article 15, GDPR).
- Control the flow of his personal data through the platform.

For other control rights (erasure and portability) regarding data which has been acquired by DSO, shall be necessary a specific request to the Data Protection Officer of the DSO, which basis additional control rights on the limits guaranteed by his legal access rights and on his additional contractual mandate which may be given to him by the end-user.

Accordingly, end-users' data protection rights (access, rectification, erasure, etc.) are all guaranteed.

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

4.2.1.1 The Privacy-by-design changes in RBAC

In the last year of the project, the RBAC in the NORM has been changed in order to reach even a higher level of privacy-by-design.

In particular, RBAC has been implemented so that it is now possible for NORM users to define a specific time period when data can be shared.

It means that **now it is possible "by-design" to pre-set the period of the data flow from NORM to DSO or other eventual subjects or components.**

This development seems to be in accordance to the so called "privacy-by-design principle".

In particular, Art. 25 of the GDPR requires that the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, (…) which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

In particular the data minimization (Art. 5(1), lett. c, GDPR) and storage limitation principle (Art. 5(1), lett. e, GDPR) require that data be collected just for what is necessary to the purpose (also considering the period of collection).

4.3 Double Virtualization and the "Data Layer"

In SUCCESS a specific mechanism for the back up of both grid and functionality data is the so-called Double Virtualization (DV) technology, which is composed of two parts: the Data Layer and the Functionality Layer.[50]

In the Data Layer are hosted grid data and Virtual Devices are hosted, virtual representation of measurement devices installed in the field, e.g., Smart Meters (SM) or Phasor Measurement Units (PMU). In other terms, in the Data Layer there can be any type of grid data that can come from the field, e.g. meter readings or voltage measurements.

The data from data layer are read by functional units from functional layer in order to execute specific function (e.g. SAU - Substation Automation Unit - provides grid state estimation; in order to do that estimation SAU should use smart meters measurements that can be identified as personal data. In order to do that, SAU (running in functional layer) will need to access to data from the database (in the data layer)

The functional and data layers, which will contain functional and data entities, will be logically separated. In case of the attack on the separate layer, the relevant entities will be migrated. In case that the attack is targeted at a single layer, its effectiveness will be reduced. Combined attacks targeting simultaneously both layers will be complex to execute, since they will require different approaches and methodologies to be applied at the same time on different targets.

We can therefore affirm that the separation between data layer and functionality layer is a form of privacy-by-design, even for the case that some kind of personal data is still used.

Furthermore, **in some cases the Functionality Layer shall need some personal data from the Data Layer**.

End-users are informed from the outset - through the specific information paper related to the contract – about this eventuality.

However, these data will be **k-anonymized**, i.e. the functionality layer will not be able to access any identifier.

[50] See Deliverable 4.4, Description of Available Components for SW Functions, Infrastructure and Related Documentation, V1 SUCCESS - Securing Critical Infrastructure, Forthcoming 2017

4.4 Three-step DPIA

Timing was an essential element to be considered for a DPIA.

As the DPIA Smart Grid Template clarifies, a DPIA should be executed **from the start of the idea 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.[51]

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 in delivering recommendations for designers and stakeholders involved in the Architecture design in month 6;[52]
2. the second step has consisted in an intermediate Data Protection Impact Assessment that has taken into account the state of the architecture design before that it was completed in month 12;[53]
3. the third step has consisted in the final Data Protection Impact Assessment after that the technology has been implemented, in month 24.[54] 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.

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

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

[53] See SUCCESS Deliverable 3.2.

[54] See SUCCESS Deliverable 3.3.

5. Conclusion: how to develop a new era for Data privacy in Energy Services

In this Deliverable we have described relevant and effective steps in order to translate Privacy Principles in practical privacy-by-design solutions.

In order to do so, we addressed 4 intermediate steps:

1. finding relative privacy principles for the power grids and energy management (Section 2);
2. translating principles in privacy guidelines for the energy sector (Section 3);
3. translating those guidelines in best practices, according to the recommendations used in SUCCESS project (Section 4);
4. translating those best practices in technical privacy-by-design solutions (Section 4).

This workflow is summarized in Fig. 4.

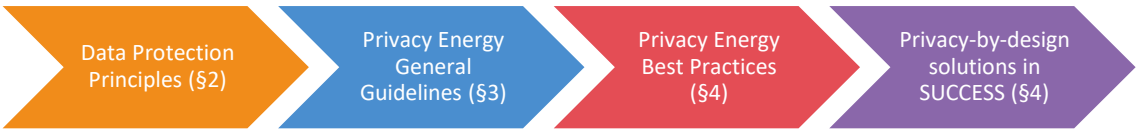

Fig. 4. The workflow from Data Protection Principles to Privacy-by-design solution in SUCCESS

Data protection principles are, e.g., data integrity, data minimization, purpose limitation, data storage limitation, lawfulness, fairness, accountability.

These principles can be well translated in guidelines for the energy sector, i.e. data access controls; prevention of unauthorized disclosures; pseudonymization; avoiding unnecessary use of personal data; aggregating data as much as possible; continuous assessment of data processing purposes and of the respect of users' rights; clear allocation of roles and responsibilities.

Such guidelines in SUCCESS have been translated into a list of "best practices" (as showed in Deliverables 2.1 and 3.1), i.e. metering data protection, anonymization of metering data, privacy preserving data aggregation, anticipated and continuous DPIA.

In more technical terms, all these best practices have been relevant for the specific design of the SUCCESS Architecture.

In particular, the whole project was based on identifying and solving Cyber-threats for smart grids and this can be for sure the best way to protect "metering data", in accordance with the "integrity and confidentiality" principle.

In addition, the Smart Meter designed within SUCCESS (called "NORM") collects personal data but does not share them with other components/agents/operator: there is an automated system (called Role Based Access Control System) through which end-users can decide who can access their data, when, how and how long. In general, however, just network data (and not consumption data) are shared, so there is no flow of personal data beyond the Utility level.

Another important solution is that access to data are controlled and logged, but since those logs are personal data (e.g., related to the physical operators of the Energy Service) there is a system of anonymization: all log data are anonymized before leaving the Utility level.

In addition, in order to enhance security of data all information is stored in a Cloud (Smart meter Gateway), but this 'virtualization of data' (called 'double virtualization') is divided into two parts: there is a Data Layer and a Functionality Layer. Data Layer (where all personal data are stored) is totally separated from the Functionality Layer. Therefore, energy operators are not allowed to access personal data if they just need data on the functionality of the network. This is a form of data minimization, though enhancing disaster recovery solutions.

In sum, conciliating cyber security and privacy can be a hard challenge within the Energy Sector. Actually, as it has been discussed in this deliverable, dealing at the same time with privacy and cyber security is an opportunity more than an issue: detecting cyber threats can be positive for data integrity; controlling access to energy data through logs can be combined with anonymization of logs at the Utility level; preparing a cloud back-up of energy data can be done separating personal data from network data.

6. 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

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

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, Privacy-Preserving Information Security Architecture

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.

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

6.1 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

7. List of Abbreviations

BMS	Building management system
BGW	Breakout Gateway
DSO	Delivery Service Operator
CI-SOC	Utility Security Monitoring Centre
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
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