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
Table of Contents

1. Introduction....................................................................................................................................... 5
   1.1. Background and Motivation ........................................................................................................ 5
   1.2. Purpose of the DPIA ..................................................................................................................... 6
   1.3. Scope of the DPIA ....................................................................................................................... 6
   1.4. Stakeholders ................................................................................................................................ 7
       1.4.1. The role of Data Protection Authority ................................................................................ 7
       1.4.2. Smart grid operator ............................................................................................................. 8
           Transmission System Operators ............................................................................................ 8
           Distribution System Operators .............................................................................................. 8
           Energy Generators (Producers) ................................................................................................. 9
           Energy Market Suppliers .......................................................................................................... 10
           Metering Operators ................................................................................................................ 10
           Energy Service Company ......................................................................................................... 10
       1.4.3. Consumer .......................................................................................................................... 11
   1.5. Benefits of performing an DPIA .................................................................................................. 12
   1.6. Carrying out the DPIA ............................................................................................................... 12
   1.7. The result .................................................................................................................................... 13
   1.8. Success factors .......................................................................................................................... 13
2. Guidance for execution of the DPIA ................................................................................................ 14
   2.1. Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA ......................... 14
       2.1.1. Criterion 1 – Personal data involved .................................................................................... 14
       2.1.2. Criterion 2 – data controller/data processor ....................................................................... 16
       2.1.3. Criterion 3 – Impact on rights and freedom ......................................................................... 17
       2.1.4. Criterion 4 - When to perform a DPIA (right timing and motivation) ................................. 18
       2.1.5. Criterion 5 – The nature of the system/application exercise ................................................ 19
       2.1.6. Criterion 6 - Legal base and public concern ....................................................................... 19
       2.1.7. Other Criterion .................................................................................................................. 20
       2.1.8. Documented conclusion ..................................................................................................... 20
   2.2. Step 2 - Initiation ....................................................................................................................... 21
       2.2.1. Organisational requirements for conducting a DPIA ......................................................... 21
           2.2.1.1. Purposes to execute the DPIA .................................................................................... 21
           2.2.1.2. The DPIA team ......................................................................................................... 21
2.2.1.3. The resources............................................................................................................. 22

2.3. Step 3 - Identification, characterisation and description of Smart Grid systems/applications processing personal data, including data flows.............................................................................................. 23

2.3.1. The use case................................................................................................................ 23

2.3.2. System Information...................................................................................................... 23

2.3.3. Description of primary and supporting assets of the system........................................ 23

2.4. Step 4 - Identification of relevant risks........................................................................ 25

2.4.1. Introduction.................................................................................................................. 25

2.4.2. Threats Identification for each feared event................................................................. 25

2.5. Step 5 - Data protection risk assessment ...................................................................... 27

2.5.1.1. Impact of feared events............................................................................................ 27

2.5.1.2. Likelihood of threats................................................................................................. 28

2.5.1.3. Final risk level / value and priority........................................................................... 30

2.6. Step 6 - Identification and Recommendation of controls and residual risks .................. 31

2.6.1. Assessment of implemented and planned controls....................................................... 31

2.6.2. Risk Treatment............................................................................................................ 32

2.6.3. Residual risks and risk acceptance.............................................................................. 33

2.6.4. Resolution.................................................................................................................. 34

2.7. Step 7 - Documentation and drafting of the DPIA Report............................................. 35

2.8. Step 8 - Reviewing and maintenance ......................................................................... 35

3. Questionnaires................................................................................................................. 36

3.1. Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA ............... 36

3.1.1. Criterion 1 – Personal data involved .......................................................................... 36

3.1.2. Criterion 2 – Data controller/data processor................................................................. 36

3.1.3. Criterion 3 - Impact on rights and freedom................................................................. 36

3.1.4. Criterion 4 – When to perform a DPIA (right timing and motivation) ......................... 36

3.1.5. Criterion 5 – The nature of the system/application exercise......................................... 37

3.1.6. Criterion 6 – Legal basis and public concern.............................................................. 37

3.1.7. Other criterion............................................................................................................ 37

3.2. Step 2 - Initiation. ......................................................................................................... 37

3.3. Step 3 - Identification, characterization and description of Smart Grid systems/applications processing personal data................................................................. 38

3.3.1. What is the detailed description of Smart Grid program/change according to M/490 Smart Grid Coordination Group use case template? ...................................................................................... 38

3.3.2. What are the main scenarios of the Smart Grid use case? ........................................ 38
1. Introduction

1.1. Background and Motivation

“A smart grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety”\(^1\).

A smart grid is supported by a communications network that collects and processes an increasingly high quantity of sensing data and makes it available to entitled stakeholders and systems. This data is collected from everywhere in a Smart Grid infrastructure, which includes consumers’ homes and possibly, electric vehicles. Smart metering systems are therefore included in this smart grid definition.

The use of smart grids and smart metering systems thus creates new risks for data subjects with potential impact in different areas (e.g. price discrimination, profiling for behavioural advertisement, taxation, law enforcement access, household security) that were previously not present in the energy sector and were more typical of, and present in other environments (telecoms, e-commerce and Web 2.0).

Smart metering is also among the first widespread applications that foreshadow the future of ‘the Internet of Things’. The risks posed by the collection and availability of detailed energy consumption data are likely to increase in the future considering the increasing availability of data from other sources, such as geo-location data, data available through tracking and profiling on the internet, video surveillance systems, and radio frequency identification (RFID) systems, with which smart metering data can be combined.

In February 2012, the mandate of the Smart Grid Task Force (SGTF) has been renewed for two years. EG2 is one of the four Expert Groups of the SGTF and is responsible for regulatory recommendations for privacy, data protection and cyber-security in the smart grid Environment.

Regarding privacy and data protection, the mandate of EG2 defined by the SGTF is to provide a Smart Grid Data Protection Impact Assessment (DPIA) template. A first template has been submitted on 8\(^{th}\) of January 2013 to the Article 29 Working Party (WP29) for consultation\(^2\) according to the point 5 of the Recommendation adopted by the Commission on the roll out of smart metering systems\(^3\). The WP29 issued its opinion on 22\(^{nd}\) of April 2013 recommending a series of changes and improvements in order for the template to be satisfactory.

\(^{1}\) Smart Grid Task Force Mandate. Brussels : European Commission, 2011.
A second DPIA template was submitted on 20 of August 2013 to the WP29 for consultation. On 4 of December 2013 the WP29 issued a second opinion recognising the work carried out by the Expert Group 2 and realising that the second version of the template constitutes considerable improvement with respect to the previous version, especially with regard to the methodology used. The WP29 also provided complementary recommendations which will contribute to the successful deployment and use of the template.

This third version of the DPIA template has been prepared by an editorial team which has constructively addressed WP29 latest recommendations and was finalised by the EG2 members on 10 of March 2014.

1.2. Purpose of the DPIA
The purpose of the DPIA is to provide guidance on how to perform a Data Protection Impact Assessment (DPIA) to Smart Grid and Smart Metering systems.

The DPIA will contribute to organisations that initiate or already manage smart grid deployments as well as those introducing changes to existing smart grid architecture platforms in identifying and assessing the privacy risks of these initiatives. In this way, organisations can take adequate measures in order to reduce these risks and, as such, reduce the potential impact of the risks on the data subject, the risk of non-compliance, legal actions and operational risk, or to take a competitive advantage by providing trust.

As such the DPIA shall be considered as complementary to, or part of, a wider risk management process an organisation has to implement and perform. Indeed, although it is called an “assessment”, the DPIA goes beyond the simple analysis of data protection risks, by describing adopted or envisaged safeguards and control measures in proportion to the risks identified, thereby being based on a risk management procedure rather than a mere risk assessment.

1.3. Scope of the DPIA
Privacy is a term that has received many interpretations over time, and often means different things in different contexts. A variety of definitions can be found and each culture and even each person has different expectations as to what constitutes an invasion of privacy. In the context of this document, the DPIA definition includes the fundamental rights defined in Articles 7 and 8 of the European Union Charter of Fundamental Rights (the 'Charter') respectively the right to privacy and the right to the protection of personal data. It should be noted that the template is related to the protection of personal data as defined in Directive 95/46/EC.

It should also be noted that data security (including cyber security) needs to be implemented in order to holistically ensure data protection.

---

Cyber security aims at safeguarding the confidentiality, integrity and availability of information assets that support vital physical assets (such as the electricity grid) against attacks, malware etc., which will disrupt the delivery of electricity.

By conducting a DPIA the following goals will be achieved:

- A DPIA 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.
- A DPIA should also help national Data Protection Authorities assess the compliance of the processing and, in particular, the risks for the protection of personal data of the data subject and the related safeguards, when data controllers consult them prior to data processing, as provided for by the Commission Recommendation. DPIAs, thus, should also assist the data controller in demonstrating compliance with Directive 95/46/EC.

1.4. Stakeholders

This part describes all the possible stakeholders involved or affected by a DPIA. The list of possible smart grid operators (see section 1.4.2) has been established based on an updated version of the list established during the first mandate of the EG2. Considering the very dynamic environment of the energy sector, this list should be considered as indicative and non-exhaustive. It will be updated on a regular basis by the European Commission.

1.4.1. The role of the Data Protection Authority

The Data Protection Authority is an important stakeholder when performing a DPIA. The DPIA report shall be prepared so that a Data Protection Authority (DPA) is able to monitor and oversee the processing of personal data, with strict respect for human rights and fundamental freedoms and guarantees as enshrined in the EU regulatory framework.

The DPIA report is provided without prejudice to the obligations set forth in Directive 95/46/EC for data controllers, most notably the independent obligation to notify the competent authority as described in section IX of Directive 95/46/EC.

The DPIA should have a clear description of all the smart grid actors, components and interactions so that the DPA is able to clearly identify the sensitivity of information being exchanged as well as all privacy-related concerns. When analysing a DPIA, the Data Protection Authority should be able to verify all identified risks and evaluate if correspondent controls are adequate for mitigation or minimization of the identified risks.

---

6 This recommendation is without prejudice to a legal obligation for prior checking in Member States, according to the characteristics of the processing operations.
7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31
8 Chapter 5, page 11 on EXPERT GROUP 2: REGULATORY RECOMMENDATIONS FOR DATA SAFETY, DATA HANDLING AND DATA PROTECTION (See http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf)
Data Controllers are encouraged to establish their duty to notify DPAs under their national law. DPIA Reports are likely to be beneficial to Data Controllers in preparing their notifications.

1.4.2. Smart grid operator

By executing the DPIA, the Smart Grid operator will be able to accomplish and prevent the following:

- Failure to comply with the relevant privacy and data protection legislation, resulting in a breach of the law and/or negative publicity;
- Stimulating public awareness or loss of credibility as a result of a perceived loss of privacy of a failure to meet expectations with regard to the protection of personal information;
- A need for systems to be redesigned;
- Contribute positively to a dialogue with the Data Protection Authority.

Under the term “smart grid operator” the following actors can be found:

Transmission System Operators

Transmission System Operators (TSOs) manage the very-high-voltage grid such as 400 kilovolt (kV) or 225 kV.

The term TSO is defined in the Electricity Directive (2009/72/EC) as a “natural or legal person responsible for operating, ensuring the maintenance of, and, if necessary, developing the transmission 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 transmission of electricity.”

Transmission ownership is decoupled from retail and generation of energy to ensure non-discriminatory access. High-voltage grids connect all regional electricity grids with each other and with the European power grid. Besides managing the high voltage grid, TSOs also monitor the reliability and continuity of the national electricity retail. Therefore, the TSO is responsible for correcting the imbalance in demand and supply in the electric power system. The TSO shall retail the balancing energy from the balancing service provider in case of shortage or surplus of electricity in the system.

In current and envisioned models it is not expected that a TSO will be involved in the processing of personal data originated from smart grids or smart metering.

Distribution System Operators

Distribution System Operators (DSOs) are responsible for energy distribution in high voltage (usually below 60 kV), medium voltage (usually between 1 kV and 30 kV) and low voltage grids.

The term DSO is defined in the Electricity Directive (2009/72/EC) as “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”.

In most European markets the role of a DSO includes being the data hub for metering data; this role will be extended by the task to manage an active power grid network that interacts with Renewable Energy Source (RES) and Distributed Generation (DG).

DSOs will be, or are already involved in the processing of personal data originated from smart grids or smart metering for the following reasons:

- DSOs will have detailed information on the status of network components, generators connected to the network and energy flows throughout the network. This includes secure remote reading of resident consumers’ metrological register(s) for all information needed for network management and quality of supply management. This information should be shared as needed to fulfil regulated duties with service providers like DG operators and aggregators.

- To avoid network congestions, local load management can reduce impacts on higher voltage levels. Local load management can also be used to enhance (local) demand response in case of relatively large uncontrollable DG. Based on their ICT systems for active network management and automatic meter reading, DSOs should develop these capabilities.

- In distribution, with massive deployment of ‘conventional’ DG and future ‘in house’ micro generation, the DSO role will gradually shift from distributing power on a top-down basis, to a role in which maintaining voltage quality and balance is central while electricity flows in both directions.

The actual implementation of this hub is dependent on the national market model which in most member states will foresee a central role for the DSO.

**Energy Generators (Producers)**

Today, bulk power generators are responsible for supplying the major share of the load, for supplying ancillary services: frequency control, voltage control, black start and reserve capacity. This role will not change in general, but with an increasing share of distributed generation, the responsibility of distributed generation in contributing to power grid stability and operational security will progressively increase.

The move towards decentralised energy production has many benefits, including the utilisation of local energy sources, increased local security of energy supply, shorter transport distances and reduced energy transmission losses. Such decentralisation may ideally foster community development and cohesion by providing income sources and creating jobs locally.

Energy generators will be involved in the processing of personal data originated from smart grids or smart metering for the following reasons:
In a smart grid environment, it is expected that decentralised energy producers may need to have access to data consumption of neighbour consumer(s) to be able to supply the area islanded from the grid or to have better voltage quality by adjusting the production to the neighbouring consumptions.

**Energy Market Suppliers**
Energy market suppliers are responsible for supplying consumers with their energy, for procuring that energy from their own sources and/or the wholesale market, for billing and serving consumers. In many Member States, such as the UK, energy suppliers are also responsible for the management of debt, for preventing and detecting theft or fraud and for providing energy efficiency advice measures and services to consumers, as well as other forms of assistance to consumers, such as in paying their bills.

Energy Market Suppliers will be involved in the processing of personal data originating from smart grids or smart metering for the following reasons:

- Handling of billing data.
- Management of debt, preventing and detecting theft or fraud.
- Providing energy efficiency advice services.

**Metering Operators**
The Metering Operator (MO) is the entity which offers services to install, maintain and operate metering equipment related to supply. This role might be split up further into two entities; one responsible to manage the meter and another for managing the metering data. In most EU Member States, the DSO is also the MO. In case of a specific contractual basis, the contract is mostly with the DSO, or may be with the consumer or the energy market supplier. The meter may be rented to, or owned by, the consumer.

Metering operators will be involved in the processing of personal data originating from smart grids or smart metering for the following reasons:

- Energy suppliers or independent companies can be responsible for reading meters and managing the metering infrastructure used by their consumers.
- Metering operators and energy suppliers may need to obtain consumption information about their consumers via the metering infrastructure with consumer consent to deliver these data to other market participants.
- DG may acquire data on energy produced and delivered to the power grid via the smart metering Infrastructure.

**Energy Service Company**
Energy Service Company (ESCo) or energy service providers are providing energy related services, e.g. energy savings advice, energy conservation, energy infrastructure outsourcing, power generation and energy supply and risk management.
ESCos initially introduced in Directive 2006/32/EC are defined in the Directive on Energy Efficiency (2012/27/EU) as “a natural or legal person who delivers energy services or other energy efficiency improvement measures in a final consumer’s facility or premises”.

Energy Service Companies will be involved in the processing of personal data originating from smart grids. The access and processing of the consumers’ data will be based on consent in principle, e.g. given when entering a contractual agreement with the ESCo.

1.4.3. Consumer

Consumers are potential beneficiaries of the execution of a DPIA as consumer data protection rights may be better served. They will of course not benefit from the assessment itself but in the actions which may be implemented after the DPIA should its report be negative. The role of the consumer is rather passive during the execution of the DPIA, unless his/her views are actively requested throughout the process. When a consumer is actively involved during this process, he may be better informed and this dialogue could positively contribute to the acceptance and deployment of the smart grid.

Depending on their characteristics, consumers could be classified into one or more of the following categories:

- **Industrial consumers**: a large consumer of electricity in an industrial or manufacturing industry. These consumers may be involved in contract based Demand/Response.

- **Building owners**: owners of a private or business building may also be involved in contract-based Demand/Response.

- **Residential consumers**: residential consumers of electricity (including agricultural users), which may be involved in contract-based Demand/Response. Within this general group, there will be vulnerable consumers or consumers who are in vulnerable circumstances that may be at greater risk of being adversely impacted by a loss of privacy.

The transition towards a decentralised energy concept reflects at least two ‘new’ types of home consumer:

- Consumers without the option of producing energy but with a potential to save energy. This will be achieved by optimisation of the home infrastructure or by means of smart living concepts.

- ‘Prosumers’ with decentralised generation (DG). The producing consumer acts as an entrepreneur and may use his DG resources by means of contracting his energy generation to service providers that pool their DG. Alternatively, he can act as a micro or individual power producer (MPP or IPP) on the basis of a contract with the local DSO.

Whether responsible parties other than the DSO (or in some countries, such as the UK, their energy supplier) should have access to consumers' specific energy usage data with a granularity of more than monthly / yearly (e.g. interval data, such as hourly) should be validated by consumer consent. In this
context it may also be necessary for both the kind and amount of data shared with those other parties to be controlled by the consumer.

1.5. Benefits of performing a DPIA

There exist a number of important benefits when performing a DPIA. The following benefits are identified when using this DPIA:

- Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks.
- Prevention of discontinuation of a project by early understanding of the major risks.
- Reducing the impact of law enforcement and oversight involvement.
- Improving the quality of personal data (minimisation, accuracy).
- Improving service and operation processes.
- Improving decision-making regarding data protection.
- Raising privacy awareness within the organisation.
- Improving the feasibility of a project.
- Strengthening confidence of consumers, employees or citizens in the way which personal data are processed and privacy is respected.
- Improving communication about privacy and the protection of personal data.

1.6. Carrying out the DPIA

When carrying out a DPIA it is recommended to use the templates that can be found in chapters 2 and 3 of this paper. The purpose of these templates is to provide guidance in the performance of a Data Protection Impact Assessment (DPIA) for Smart Grid and Smart Metering systems. It describes a documented process comprising the following important steps:

- Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA;
- Step 2 - Initiation;
- Step 3 - Identification, characterisation and description of smart grid systems / applications processing personal data;
- Step 4 - Identification of relevant risks;
- Step 5 - Data protection risk assessment;
- Step 6 - Identification and recommendation of controls and residual risks;
- Step 7 - Documentation and drafting of the DPIA Report;
- Step 8 - Review and maintenance.

In chapter 3, tables and templates are provided to support these steps (up to step 6). Explanation and details for each step are provided in chapter 2.
1.7. **The result**
By following the above-mentioned steps, the DPIA should help stakeholders to identify in a structured way and to categorize privacy risks attached to smart grids systems and applications when processing personal data. Furthermore the template will help mitigate risks by defining the necessary process steps to find appropriate controls attributed by examples of controls measures. The result of the DPIA is a report that gives a valuable basis for decision making.

1.8. **Success factors**
The following factors can contribute to a successful DPIA:
- A DPIA is not an ad-hoc or random exercise. The DPIA is an integral part of risk management and/or has a structural place in projects, programs or processes;
- A DPIA is performed at an early stage (preferably during the design of new applications or systems);
- During the DPIA relevant internal and external stakeholders are actively involved;
- DPIA’s are future oriented to support the identification of privacy risks before the usage of new applications or implementation of new programs;
- The DPIA is not used as a static document and is adjusted during a project (especially when privacy risks are changing);
- The DPIA is preferably performed by a multidisciplinary team of experts;
- The DPIA is part of a system of motivating, sanctioning and controlling;
- The DPIA is part of the quality assurance process of a project methodology;
- The team performing the DPIA has both knowledge of the project/program and access to relevant expertise concerning privacy;
- External stakeholders are involved during the DPIA;
- There is a (formal or informal) process to control the result of a DPIA by external/independent persons.
2. **Guidance for execution of the DPIA**

This chapter describes the steps to be taken when carrying out a DPIA. Furthermore, this chapter can be used as an exploratory chapter to the DPIA template of chapter 3. Having chapters 2 and 3 presented side-by-side (with two screens or with two printed copies) might facilitate the understanding of the DPIA process and streamline its accomplishment.

2.1. **Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA**

The objective of this section is to provide guidance to the system owner of a smart grid system to determine if a DPIA is necessary and who should conduct this DPIA. It is therefore proposed to the system owner to perform an initial analysis of the application under consideration and to decide whether to proceed with the next steps of the DPIA or to stop the process.

During this step the questions in section 3.1 should be answered. Positive replies endorse the need to carry out a DPIA. This is not a quantitative exercise. This means that a single positive answer might make it necessary to conduct a DPIA.

When answering the questions in section 3.1, the following criteria might be considered.

2.1.1. **Criterion 1 – Personal data involved**

The purpose of this section is to get an initial insight of the data collected and used and the potential necessity to execute a DPIA. The concept of personal data is defined in article 2 of the Directive 95/46\(^\text{10}\). Further guidance regarding this definition can be found in WP136 opinion of the Article 29 Working Party on the concept of personal data\(^\text{11}\).

It should be underlined that when processing personal data, it should be considered whether it is absolutely necessary for operational purposes. If not, personal data processing should be avoided whenever possible.

Specifically, for smart grid applications, non-exhaustive examples of personal data would be:

- Household and organisations 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 subject;
- 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;
• Facility operations profile data (e.g. hours of use, how many occupants at what time and type of occupants);
• Frequency of transmission of 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

Illustrative example 1:
The utility makes a website available that allows the consumers to access their consumption data online. The consumers have to subscribe to this service and give their consent. The personal data – by definition - has to be transmitted from the smart meter to the central systems in a secure way in order to mitigate to a satisfactory level the risk of a possible breach.

Illustrative example 2:
Smart meters register consumption data every 15 minutes (configurable). The data concentrator collects these 15 minutes readings once a day and sends them back to the backend systems. These readings might be considered private information in such a way that they can be illegitimately used to assess sensitive information regarding the behaviour of each client.

Illustrative example 3
Implementing smart charging of EVs calls for an interaction and corresponding information exchange between DSOs, Charge Spots, EVs, EV drivers and new market participants. One could add a Charge Service Provider (CSP) who deals with fulfilling the charge wish of the EV driver and a Charge Spot Operator (CSO), who deals with the operation of the Charge Spots. Without measures, one could derive the charge locations of an EV throughout time. If this could be coupled to an EV driver, it would then become personal data as it reveals the whereabouts of the latter. Without taking into account the privacy concerns, this might lead to a lower acceptance of EV and smart charging.

Non personal data:
• Household frequency, voltage etc. (no link to consumer behaviour);
• At feeder, transformer or network levels (no link to individual consumers and their behaviour. Consumption, frequency, voltage etc.).
Illustrative example 4:

An energy supplier maintains a list of systems and versions provided (e.g. leased) to a micro grid operator. This data will not be considered as personal data.

Illustrative example 5:

Technical data and commercial information are stored and processed in different systems. The common key (also called primary key) that is used to link the two types of data is location (the address). This way, client’s personal data is better protected as it is not directly available when accessing technical data only.

2.1.2. Criterion 2 – data controller/data processor

The system owner also needs to clarify if he can be considered as a data controller. Indeed, if a smart grid application/system operator makes determinations related to the collection or use of personal data, its role could be similar to that of the Data Controller as defined in Directive 95/46/EC and would be described as the natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes, conditions and means of operating such smart grid application/system which has impacts on personal data.

The application/system owner should determine and clarify already at this stage if he can also be considered as a data processor who conducts the identified processing operations on behalf of the data controller. He might then suggest to the Data Controller to conduct a DPIA and assist him in this task within the limit of his responsibility.

These two roles are defined by article 2 d) and e) of Directive 95/46 and further guidance can be found in tWP 169 opinion of the Article 29 Working Party on the concepts of controller and processor.

Illustrative example 1:

An energy supplier and an insurance company work together to provide insurance that covers stability of energy supply for micro-grid operators. In order to assess applicability of coverage, monitoring in energy supply is implemented. The respective role and responsibilities of all parties involved need to be made clear.

As in most member states, the DSO is the metering operator and as such, the DSO is the data controller in the first part of the metering data process (DSO’s process ends with creating a bill for network usage; in a second step the metering data is being passed on to the supplier who will create a bill for the electricity supplied). The DSO can outsource parts of his metering business to a data processor (e.g. reading out meters, delivery of meter data to DSO). In this case, the outsourcing partner/data processor could become part of the DPIA whereas the supplier has to conduct an individual DPIA himself (DSO’s responsibilities end by passing on the metering data to the supplier).

When cloud computing infrastructures are used or envisaged, the determination of the controller/processor might be more difficult to achieve and conducting a DPIA in this case will facilitate this clarification.

2.1.3. **Criterion 3 – Impact on rights and freedom**

The organisation should determine whether the processing operations present specific risks to the rights and freedoms of the data subject by virtue of their nature, their scope or their purposes. In this preliminary step the aim is not to conduct a full risk assessment as foreseen in step 3 of the DPIA process, but more to list the ones which could already be envisaged considering the nature of the personal data processing.

Profiling of individuals, targeted advertisement and any other added-value services based on detailed analysis of the energy use behaviour could constitute illustrative example for this part (listing them in this part does not mean at all that they are not recommended or even forbidden but that they should trigger a DPIA).

The following risks can be considered as specific ones which will trigger the need for a DPIA:

For the individual,

- Loss of independence (e.g. by preventing to provide own energy supply);
- Loss of equality (e.g. by difference in approaching individuals based on consumption or production);
- Stigmatization (e.g. by judging if someone has a clean/green energy supplier or not);
- Loss of freedom to move (e.g. not able to load an electric car);
- Interference with private life (e.g. incidentally cut-off energy supply by wrong decision based upon quality of data);
- Manipulation (e.g. by threat to cut off energy supply by individual or organisation);
- Loss of Autonomy (e.g. by not being able to live by their own standards).

<table>
<thead>
<tr>
<th>Illustrative example 1: Individual reading information is processed in the data collector (should be either aggregated or based on PET)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Illustrative example 2: Individual reading information circulates unencrypted through the SG infrastructure</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Illustrative example 3: Client smart meter readings are available through the supplier website.</th>
</tr>
</thead>
</table>
2.1.4. Criterion 4 - When to perform a DPIA (right timing and motivation)

**Right timing**

In the case of the development of a new application or system, in compliance with the principle of privacy by design, 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.

With already existing applications the following criteria should also be considered when envisaging a DPIA:

- Significant changes in the smart grid application, such as material changes that expand beyond the original purposes (e.g., secondary purposes);
- Processing of new types of information;
- Unexpected personal data breach with significant impact and the occurrence of which had not been identified in the residual risks of the application identified in part 5 of the first DPIA;
- The system owner in accordance with the risk management policy might define periods of regular reviews of the DPIA report;
- Substantive or significant internal or external stakeholder feedback or inquiry;
- Use of cloud based services for processing personal data issued from the smart grid system;
- In the context of change management procedures such as material changes that expand beyond the original purposes (e.g., secondary purposes): throughout the lifetime of the Smart Grid application, a new or revised DPIA Report should be warranted if there are technological-related changes in applications, etc. that may have data protection implications for the smart grid application under consideration.

Indicators demonstrating that adequacy or compliance of existing systems are not in line with latest standards or insights (e.g. systems that have not been built with data protection by design in mind) constitute trigger elements for conducting a DPIA. On the other hand, material changes that would narrow the scope or minimize the collection or use of personal data would not per se trigger the need for a revised DPIA as they should decrease the risks already identified and approved.

**Motivation**

A DPIA process may be motivated by the following elements:

- A willingness to prevent costly re-design and control risks when designing and implementing smart grid (components);
- The necessity to ensure compliance with data protection and security legislation as well as other relevant legal obligations. It is already the case for specific organisations in some Member States. It is also envisaged in the proposed Reform of the General Data Protection legislation (Article 33 of the Regulation)\(^{13}\) to be mandatory under certain conditions;

• As part of a wider risk management process (e.g. ISO 27005). Using a DPIA, data protection issues might be considered in the risk identification and assessment;
• Corporate rules and culture;
• Accountability and communication policy sometimes related to the previous point with the aim of obtaining certification/seal.

This initial analysis and the decision (not) to conduct a DPIA has to be documented and may assist a company in case it is subject to an investigation by data protection authorities.

In case of doubt regarding the results of this analysis and the decision to be adopted, the organisation should consult the Data Protection Authorities according to national practices.

2.1.5. Criterion 5 – The nature of the system/application exercise
The main question which should be addressed by the system owner is: what is the nature of the application or system?

What components/functions of the application will be considered in the scope? The idea of this criterion is not to reproduce in detail the step 3 of the DPIA process but to provide a first overview of the possible perimeter of the application at stake. This step will provide an initial insight in the system and potential necessity to execute a DPIA.

2.1.6. Criterion 6 - Legal base and public concern
The processing of personal data is regulated by the EU legal framework (Directive 95/46/EC) transposed by Member States\textsuperscript{14}. The word 'processing' means any operation or set of operations performed upon personal data or 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, erasure or destruction. The system owner of the application needs to determine if at least one of these operations is implemented and how far the organisation has control on it (see criterion 2).

The choice of the legal basis for these processing operations has to be carefully selected and duly justified. Article 7 of Directive 95/46/EC offers a series a possible legal basis which might be applied. Further guidance on the processing of smart metering data and compliance with the Data Protection Directive can be found in Article 29 Working Party opinion WP183\textsuperscript{15} on smart metering.

The non-exhaustive list below provides some illustrative examples of processing of personal data.

• Reading out a meter manual/remote, entering data into database;
• Storage of meter data in meter or telecommunication device incl. intermediate storage;
• Adding meter data to tariff registers in the meter and/or back end systems,

\textsuperscript{14} http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
\textsuperscript{15} http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf
• Transfer of meter data / tariff register data via WAN to a back end system naming addressing, encryption, data plausibility mechanism (e.g. detecting tampered data);
• Applying tariffs to the meter data, e.g. multiplication of annual consumption with price/kWh in the back end system;
• Creating a bill out of the aforementioned data (Billing data).

Following the Article 29 Working Party opinion WP205, it could be stated that the following processing operations do not request user consent and might be triggered by the legal obligations of the smart grid operator:

• the provision of energy,
• the billing thereof,
• detection of fraud consisting of unpaid use of the energy provided,
• Preparation of aggregated data necessary for energy-efficient maintenance of the grid (forecasting and settlement).

On the other hand, tracking and profiling processing operations for the purpose of targeted advertisement will require a freely given, specific, informed and explicit consent.

Illustrative example 1:

The advanced smart grid functionality of load balancing requires data collectors to have near real time access to the mapped meters readings to be able to efficiently manage energy production and consumption, including micro generation and distributed generation. The Smart Meter readings are critical for the processing of the smart grid response for a load balancing event using the described strategy of near real time data collection on meter level.

2.1.7. Other Criteria
Besides the above mentioned criteria there could be other reasons to execute a DPIA. These should be identified.

2.1.8. Documented conclusion
At the end of this section a documented conclusion identifying whether a DPIA is needed or not should be produced based upon the answers to the questions. This should be endorsed by the management.

Expected deliverables for this preliminary step: a documented decision endorsed by higher management on whether or not the organisation shall conduct a DPIA

---

2.2. **Step 2 - Initiation**

When initiating a DPIA different elements should be considered. The table in section 3.2 should help by documenting the necessary information.

2.2.1. **Organisational requirements for conducting a DPIA**

Before describing the process itself, this document presents a non-exhaustive series of organisational guidelines which will contribute to the success of a DPIA. These guidelines have been drafted based on several guidelines on Privacy Impact Assessment in Europe\(^{17}\) as well as the expertise of the EG2 members in the field of risk management.

2.2.1.1. **Purposes to execute the DPIA**

The DPIA can be used in different ways for different purposes by different types of persons. Use of the DPIA will provide them with answers to different questions such as:

**Investor / Management / Project initiator / system owner**
- Will the investment be realistic from the viewpoint of data protection?
- Are the risks known and can they be mitigated?

**Project management**
- Are non-functional requirements sufficiently dealt with?
- Are the risks known and are we (still) dealing with them?

**Compliance and oversight functions**
- Is the risk assessment properly executed?
- Are all stakes of stakeholders dealt with and balanced?

**System developers / project executions**
- What measures do we need to take?
- What are the boundaries for performing the work?

2.2.1.2. **The DPIA team**

Three possible options for the management of the DPIA should be envisaged, each of them having its merits and drawbacks:

1. A dedicated team within the organisation but not the one in charge of the application. The Data Protection Officer should be involved or contribute to this team from an evaluation or an operational point of view:
   a. Persons with knowledge of the automation environment (hardware, software, networks and network components);
   b. Persons in the user environment;

2. A third party providing external expertise needed for the DPIA;

\(^{17}\) [http://www.piafproject.eu/](http://www.piafproject.eu/)
3. The persons in charge of the application/system which is the target of the DPIA. This might especially apply in the case of SMEs with limited resources.

When the resources of the organisation allow it, option 1 should be favoured. The team conducting the DPIA should be as independent as possible from the team working on the smart grid application itself.

The DPIA team requires strong understanding of the project itself, knowledge of privacy, data protection and cyber security and expertise in the performance of risk assessments generally and privacy impact assessment in particular. Because of the diversity of expertise and interests involved, it is common to conduct the DPIA with a small and multidisciplinary team where the following expertise is combined:

- Risk assessment;
- IT architecture and system engineering;
- Information security;
- Privacy and data protection;
- Legal;
- Organisational design;
- Project management.

2.2.1.3. The resources
A key success factor for the success of the DPIA is the support of higher management. If higher management does not give the necessary support, the workload and time could be increased and the results can be disputed or disregarded.

The necessary resources that will be used in order to execute the DPIA will be obtained through interviews or available documents such as:

- Project documents such as project plan, project initiation document, business case;
- Architectures, such as IT and enterprise architectures;
- Requirements documentation, such as functional, technical and non-functional requirements;
- Type of data to be generated and its purpose of use;
- Contracts with system engineers, IT hosting parties, IT service providers, installation and service providers;
- System design documentation, such as interface design, communication protocols.

The outcome will be a good understanding and description of the data flow and the parties and systems involved in that data-flow as well as the data protection and security measures envisaged.
2.3. Step 3 - Identification, characterisation and description of Smart Grid systems/applications processing personal data, including data flows

In this step, the system owner should give a comprehensive and full picture of the application, its environment, processed data and system boundaries. The application design, its adjacent interfaces with other systems, and information flows are to be described.

Data flow diagrams that show processing of primary and secondary data are recommended to visualize origin, locations and destination of data. Data structures need to be documented too, so that potential links can be analysed. In order to accomplish these, the system owner will be invited to fill in a set of tables as they go through the template. Each table is accompanied by a set of instructions about how it should be filled in order to provide guidance through this part of the process.

2.3.1. The use case

The aim of the template in section 3.3 is to gather relevant and overall information regarding the processed data, the use case, the organisation, actors involved, the system owner, and the project. Introduced at the beginning of the DPIA, this table should be completed and finalised at the end of the process. The system owner should refer to the document\(^ {18}\) prepared by M/490 smart grid coordination group for assistance in order to complete the use case template description in a standardised way.

All roles and responsibilities in relation to personal data processing operations need to be clearly documented and, when necessary, communicated.

2.3.2. System Information

The system owner should fill-in this table with the requested information in order to characterise the targeted smart grid/ smart metering application. It should be filled with “NA” when the field in question is Not Applicable to the application; not already listed objectives that are specific to the application should also be included in this table.

2.3.3. Description of primary and supporting assets of the system

Each system identified in the tables should be described including workflows of personal data (the categories of data subjects and category, nature of the process, the recipient to whom data may be disclosed, how information is provided to the data subject, retention policy, technology uses, communication protocols uses, etc.). A clear description of the data flows, including the primary assets on which the processing of personal data rely on (e.g. a database acting as a repository of the data collected in a certain area) should be provided.

For each processing of personal data, primary assets are the following:

- **processes**: those of the processing operations specific to smart grid management dealing with personal data and those required by Directive 95/46 and listed in Annex I “Privacy and data protection targets” (for example the data subject’s right of access or right to object require specific processing operation which need to be described)

- **personal data**: those directly concerned by the processing operations necessary for the management of the smart grid and those concerned by the processes required by the Directive 95/46 and listed in Annex I “Privacy and data protection targets”.

It is of great importance that the legal basis for these processing operations is clearly identified and presented in detail, and for those of them requiring the consent of the end-user, the process for obtaining this consent needs to be documented as well as the process foreseen for the withdrawal of consent. These processes are considered as well as primary assets to be appropriately protected.

These primary assets rely as well on various information system components considered as supporting assets which include the following elements:

- **Hardware**: computers, communications relay, USB drives, hard drives, sensors, smart meters, remote terminal units (RTU), intelligent electrical devices (IED), actuators, data concentrators, servers, front-ends, work stations
- **Software**: operating systems, messaging, databases, business applications, Advanced Metering Infrastructure (AMI) Head-end...
- **Networks**: electricity and data cable, wireless, fibre optic, routing and switching devices
- **People**: users, administrators, top management...
- **Paper media**: printing, photocopying, invoices, delivery contracts...
- **Paper transmission channels**: mail, workflow..., personalised web-portals

The system owner should pay great attention to the description of the primary and supporting assets as they will provide, in addition to the list of controls, the main input for the risk evaluation step.

**Expected deliverables for this step**: A detailed inventory of the primary and supporting assets of processing operations is established, together with any contribution thoroughly describing the system and application.
2.4. Step 4 - Identification of relevant risks

2.4.1. Introduction

The goal of this step is to identify the conditions and potential risks that may threaten or compromise personal data of the data subject and impact his/her privacy using the EU Directive as a reference for important hallmarks of privacy and data protection targets to protect.

A risk assessment process should typically consider the risks of a smart grid Application in terms of their likelihood of occurrence (likelihood) and the impact of their consequences (severity). These privacy risks are mainly constituted by a feared event and the threats which might trigger these events (several threats can trigger the same feared event). Whenever available within the organisation, the Data Protection Officer should take part in this analysis as already suggested in 2.2.1.2.

The feared events represent the following situations to be avoided:

- Unavailability of legal processes: they do not or no longer exist or work;
- Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection...);
- Illegitimate access to personal data: they are known by unauthorized persons;
- Unwanted change in personal data: they are altered or changed;
- Disappearance of personal data: they are not or no longer available.
- Diverting of personal data to other users: they are distributed to people that have no need.

Whenever these events will take place, they will have impacts on the privacy of the data subjects and these impacts need to be properly and systematically assessed and ultimately mitigated.

Accidentally or deliberately, these feared events will be triggered by one or more risk sources, mainly the following:

- Insider: persons who belong to the organisation: user, system operator, grid operator, service operator, call centre operator, commercial service employee
- Outsider: persons from outside the organisation: recipient, provider, competitor, authorized third party, government organisation, human activity surrounding, external/sub-contracted maintenance
- Machine: non-human sources: corrupt sensor, computer virus, natural disaster such as lightning, energy imbalance, energy disruption an outage.

2.4.2. Threats Identification for each feared event

Starting from the analysis performed in step 3 (description of the system), threats can be identified for each feared event described above. The aim is to establish, for the system which is under the scope of this assessment, a detailed and prioritized list of all threats that would trigger these feared events.
In 3.4.1 a list of potential threats and specific energy industry examples are listed. This non-exhaustive list need to be made applicable and tailored to your circumstances. The list of threats and the answers to the questionnaire in 3.4.1 should provide guidance on the identification of the threats related to your system.

The system owner should select an appropriate internal numbering system for the ID of the threats in order to allow the reviewer of the DPIA report to uniquely identify given threats.

**Expected deliverables for this step:** A detailed inventory (see proposed table in part 3.4.2) of the threats related to the primary and supporting assets of processing operations identified in the previous step and triggering specific feared events.
2.5. Step 5 - Data protection risk assessment

In this step the identified feared events and related threats will be weighed with the severity of impact on the individuals and likelihood of occurrence. In order to classify the impact and likelihood, several widely available models can be used.

The illustrative model for classification which is proposed and detailed below is mainly based on ISO 31 000, EBIOS methodology and the synthesis produced by the CNIL\(^{19}\), the French data protection authority.

However, it is acceptable to use alternate methodologies; either industry standard or internal ones as long as the privacy risks which can impact the data subject are properly identified and quantified.

2.5.1.1. Impact of feared events

The feared events are ranked by determining their impact and severity based on the level of identification of personal data and the prejudicial effect of these potential impacts. This potential impact is defined by the consequences each feared event could have on a data subject's privacy and other fundamental rights and freedoms, including e.g. crime related risks such as identity theft and fraud, or freedom to move, independence, equal treatment, social relationships, financial interests, etc. due to e.g. profiling, unsolicited marketing, discrimination or individual decisions on wrong information. The consequences of feared events may not impact all data subjects equally. Vulnerable consumers or consumers in vulnerable circumstances may be more adversely affected by privacy risks than consumers generally, so it is important that the assessment reflects the greater impact relating to specific consumer groups.

When assessing the impact and severity of a certain identified threat, the following elements need to be considered.

- The privacy targets (see Annex I)
- Crime related risks such as identity theft and fraud
- Impact on other privacy principles such as freedom to move, loss of independence, loss of equality etc. due to e.g. profiling, unsolicited marketing, discrimination or individual decisions based on wrong information.
- The potential impact from feared events may extend beyond those consumers who are directly affected and this should also be considered in the impact assessment.

The first step to conduct is to assess the level of identification of all personal data established beforehand in the list of primary assets. In other words, how easy is it to identify data subjects with the available data processed by the system?

1. **Negligible**: Identifying an individual using their personal data appears to be virtually impossible (e.g. searching throughout a Member State population on one meter reading).

2. **Limited**: Identifying an individual using their personal data appears to be difficult but is possible in certain cases (e.g. searching throughout a Member State population using an individual's 1 day history of meter readings).

3. **Significant**: Identifying an individual using their personal data appears to be relatively easy (e.g. searching throughout a Member State population using an individual's history of meter readings of multiple days).

4. **Maximum**: Identifying an individual using their personal data appears to be extremely easy (e.g. searching throughout a Member State population using an individual's history of meter readings).

The value of the level that best matches the personal data identified is then selected. Any existing or planned measures that reduce the identification should be documented and will be taken into account in the next step (Step 6 on controls and final risk level).

The prejudicial effect of each feared event should then be estimated. In other words, how much damage would be caused by all the potential impacts?

1. **Negligible**: Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).

2. **Limited**: Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).

3. **Significant**: Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).

4. **Maximum**: Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

The value of the level that best matches the potential impacts identified is then selected. Any existing or planned measures that reduce the prejudicial effect should be documented and will be taken into account in the next step (Step 6 on controls and final risk level).

The last step of this process is to determine the severity/impact of the feared events and their related threats. It is accomplished by adding the number obtained with respective personal data level of identification and the number of prejudicial effects of potential impacts values obtained (a table is provided in part 3.5).

2.5.1.2. **Likelihood of threats**

The likelihood will be assessed by the combination of the level of vulnerability of the supporting assets and the capability of the risk source for the exploitation of this vulnerability.
First, the vulnerabilities of the supporting assets are estimated for each threat identified previously. In other words, to what degree can the properties of supporting assets be exploited in order to carry out a threat?

1. **Negligible**: Carrying out a threat by exploiting the properties of supporting assets does not appear possible (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
2. **Limited**: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult (e.g. theft of paper documents stored in a room protected by a badge reader).
3. **Significant**: Carrying out a threat by exploiting the properties of supporting assets appears to be possible (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at reception).
4. **Maximum**: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy (e.g. theft of paper documents stored in a lobby).

The value of the level that best matches the supporting asset vulnerabilities identified is then selected. Control measures which are already implemented or planned for the system/application and which should in principle reduce these vulnerabilities and impact the value of this level will be taken into account in the next step (Step 6 on controls and final risk level).

Then the capabilities of risk sources to exploit vulnerabilities (skills, available time, financial resources, proximity to system, motivation, feeling of impunity, etc.) are estimated for each threat.

1. **Negligible**: Risk sources do not appear to have any special capabilities to carry out a threat (e.g. software function creep by an individual acting without malicious intent and who has limited access privileges).
2. **Limited**: The capabilities of risk sources to carry out a threat are limited (e.g.: software function creep by a malicious individual with limited access privileges).
3. **Significant**: The capabilities of risk sources to carry out a threat are real and significant (e.g. software function creep by an individual acting without malicious intent and who has unlimited administration privileges).
4. **Maximum**: The capabilities of risk sources to carry out a threat are definite and unlimited (e.g. software function creep by a malicious individual with unlimited administration privileges).

The value of the level that best matches the risk sources identified is then selected. Any existing or planned measures that reduce the capabilities of risk sources should be documented and will be taken into account in the next step (Step 6 on controls and final risk level).

The last step is to determine the likelihood of the identified threats by summing the values obtained for the vulnerabilities of the supporting assets and the one related to capabilities of the risk sources (a table is provided in part 3.5).
2.5.1.3. Final risk level / value and priority

Once the relevant threats have been identified, their quantification will lead to risks related to the feared events which should be considered from the point of view of their impact/severity and likelihood (as highlighted above). Risks should be presented in order of priority. According to their respective levels, they can require additional measures as explained in the next step (step 6).

If not already documented, this should also include details of the impacted part of the application/system and stakeholders which should have been listed in the description.

The order of priority for the identified and quantified risks should lead to the following statement:

1. **Risks with a high severity and likelihood** must absolutely be avoided or reduced by implementing security measures that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that these risks are treated by independent measures of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).
2. **Risks with a high severity but a low likelihood** must be avoided or reduced by implementing security measures that reduce either their severity or their likelihood. Emphasis must be placed on preventive measures.
3. **Risks with a low severity but a high likelihood** must be reduced by implementing security measures that reduce their likelihood. Emphasis must be placed on recovery measures.
4. **Risks with a low severity and likelihood** may be taken, especially since the treatment of other risks could also lead to their treatment.

The different actions for this assessment can be summarised as below:
Illustrative example: a feared event A with 2 points for identifiability and 1 point for prejudicial effects will get 3 points for severity.

Expected deliverables for this step: A completed table as provided in paragraph 3.5 together with a mapping of the identified risks within the map provided. At this stage, the controls and mitigation measures implemented and planned are still not taken into account in the evaluation level of risks.

2.6. Step 6 - Identification and Recommendation of controls and residual risks

2.6.1. Assessment of implemented and planned controls
At this stage, the aim is to consider the risks identified and assessed in the previous step and to present which controls have been implemented or are planned to be implemented in order to reduce the risk at appropriate levels. Each identified risk needs to be appropriately mitigated by one or more controls considering their likelihood and impact. In Annex II an indicative list of possible controls is provided. The EG2 is establishing a list of ‘Best Available Techniques’ in smart metering system environments which can provide further guidance to the data controller regarding which control will be the most efficient.
Best Available Techniques, as defined in the point 3.f of the Recommendation\(^{20}\), refers to “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.”

The controls adopted or already planned by the system owner should cover the following dimensions:

- The infrastructure (communication network, Equipment Protection, hardening, etc.);
- The agents/personnel involved in the process (Individual access and control mechanism, etc.);
- The organisation and procedure (Smart grid application governing practices, accountability measures, etc.);
- The technologies (system protection measures including Security Controls and IT based security methodology, etc.).

The DPIA report should explain in detail how the selected (implemented or planned) controls relate to specific risks, and should demonstrate that they result in acceptable risk levels. When the risk is shared with a third party, the system owner should also detail which control this third party has implemented or planned to implement in order to address this risk in an acceptable way.

It is also recommended to design and implement an internal process (see step 8) with the aim of regularly verifying if identified controls are in place (e.g. performing audits on a regular basis, which is the ultimate control listed in the List of Controls in Annex II).

Expected deliverables: A list of planned and implemented controls for mitigating the identified risks and a new risk map with location of residual risks (part 3.6) In principle this new risk map should have residual risks at a lower level compared to the first risk map with no controls.

### 2.6.2. Risk Treatment

Having identified and assessed the risks, the system owner needs to specify the way in which these risks will be managed. This can be done with the inclusion of a new column as proposed in table of part 3.6. In this column, the system owner should also describe the way the privacy targets as defined in Annex I have been implemented, OR provide a justification if they have not been implemented. The possible options which can be adopted to manage those risks are proposed below:

- **Risk Modification**: The risk is managed by identifying and introducing additional (to those already implemented or planned and described in section 2.6.1) appropriate controls, thereby reducing the risk to acceptable levels;
- **Risk Retention**: The system owner accepts the risk as it is, if it meets the acceptance criteria, without any further action;
- **Risk Avoidance**: The system owner decides not put the application in production;

---

\(^{20}\) Commission recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (COM 2012/148/EU)
• **Risk Sharing:** The risk is shared with a third party, which can manage the identified risk more effectively and thereby reduce the risk at acceptable levels.

It is noted that these options are not mutually exclusive. The system owner may decide to go with more than one option. Further details should be added to the report regarding the approach undertaken. The following information should be at least included:

- Appropriate justification for the selection of specific option(s) for treating the risk and proposed approach to ensure that the risk will be monitored to make sure acceptance is appropriate in light of the evolving external landscape (e.g. threats, vulnerabilities, legal requirements etc.). Ideally the system owner should perform a cost benefit analysis when selecting among these option, considering the expected benefits and costs of implementing each option;
- Consultation of the Data Protection Officer (DPO) when available;
- Date: The decision was approved (this should include history demonstrating each time the action was taken);
- Date of next review if already planned;
- External Review: Any details of this document being reviewed (with comments) from third party review.

### 2.6.3. Residual risks and risk acceptance

According to ISO 27005, the residual risk is “the risk remaining after the risk treatment”. In this context, the system owner needs to appropriately identify the residual risks that remain after implementing controls. When those are identified (in the previous step), the system owner would then need to decide whether additional controls would need to be implemented to address those residuals risks considered as still unacceptable.

Finally, based on this analysis and the acceptance levels set by the management, the decision to accept those risks may need to be made. The decision should be appropriately and carefully justified, especially in the case of risks that don’t fall within the acceptable levels and that are accepted (e.g. because it is not considered cost-efficient to address them, in view of the advantages associated with the risk etc.). The system owner needs to demonstrate that the benefits of processing greatly outweigh the risks for the individual.

It should be reminded that the right for the protection of personal data is a fundamental right and compliance with it is a high-level legal requirement. Independently of the outcome of this risk assessment, it has to be underlined that data protection and privacy targets (listed in Annex I) have to be reached. For example the processing operations always need to be supported by a lawful ground.

An unencrypted data exchange which had a high risk of privacy breach is addressed by implementing a cipher suite in the platform to ensure confidentiality. However, due to technology and cost limitations the encryption algorithm is not that strong and proven to be vulnerable to brute force attacks. The initial risk has been addressed; however, there are still residual risks. For instance, the implemented control itself may be broken. Over time it may happen that the encryption algorithm becomes less secure and will therefore impact the level of the residual risk. The likelihood of this happening increases in time.
### 2.6.4. Resolution

The resolution of the DPIA should be based on the results of the risk management process that has been performed, as well as on the residual risks and the decision to accept risks or not (based on a cost-benefits analysis as well).

A smart grid application/system will be considered by the system owner as satisfactory once the DPIA process has been completed with relevant risks identified and appropriately treated to ensure no unacceptable residual risks for the individuals remain, and in order to meet the requirements of compliance, with appropriate internal reviews and approvals.

The following resolutions can be envisaged at the end of the DPIA process:

- A smart grid system or application already in production:
  - The DPIA is positive: The DPIA reports should be registered and stored by the Data Protection Officer (if any) of the organisation and kept at the disposal of the Data Protection Authority
  - The DPIA is negative: further consideration will require a specific corrective action plan to be developed including proposal for more efficient or new controls, and a new DPIA to be completed in order to determine if the application has reached an approvable state.

- A smart grid system or application still under design:
  - The DPIA is positive: risks have been assessed and controls addressing those risks properly defined and tuned. Any residuals risks have been flagged and no further controls have been identified and / or certain risks have been accepted. The system implementation proceeds. The DPIA report should include future dates for checking the system when it will be in production.
  - The DPIA is negative: in addition to envisaging further controls for obtaining a new and satisfactory level of residual risks, the report should also recommend when possible, new design actions for the application following the principle of Privacy by Design.

It is important to note that the final resolution should be a management decision and it should be based on the results of the assessment performed, including and reflecting the societal stakes related to the development of the smart grid.
2.7. **Step 7 - Documentation and drafting of the DPIA Report**

The performance of the DPIA following the phases identified above should be appropriately documented and its results presented in the final DPIA report. The DPIA report can be structured around the phases of work described in this document, presenting the results of each phase to the reader, annexing any supporting documents or material used in the assessment.

The objective of the documentation is two-fold: (a) to facilitate the implementation of the process and (b) to produce a final report that could be submitted to the DPA if requested.

DPIAs are internal processes and may handle proprietary classified information of the organisation related to products and processes, with special confidentiality requirements. As such, the analysis performed and its documentation may need to be appropriately secured, in accordance with the organisation’s information classification scheme.

The signed DPIA Report that contains an approved resolution should be given to the assigned organisation’s Data Protection Officer (if any\(^\text{21}\)) in accordance with the system owner’s internal procedures. This report is provided without prejudice to the obligations set forth in Directive 95/46/EC for data controllers, most notably the independent obligation to notify the competent authority as described in section IX of Directive 95/46/EC.

In the resolution, the data and the name and title of the person signing should be clearly included.

| Expected deliverables for this step: | The DPIA report, which can be distributed to stakeholders when appropriate. |

2.8. **Step 8 - Reviewing and maintenance**

The purpose of this phase is to ensure that the undertaking arising from the conducted DPIA are carried out in the existing system(s) or implemented project.

The following tasks are suggested:

- Reviewing the implementation of the mitigation and avoidance controls that were identified in the DPIA;
- Preparing a review report;
- Presenting the privacy review report to the senior management and DPO where available;
- Rendering the privacy review report publicly available;
- Assessing whether there is a need for revising the DPIA after a certain amount of time or after a new stage within the project or programme has been completed.

The review can be integrated within the organisation’s standard, periodic or occasional internal processes.

\(^{21}\) In Germany there are legal obligations to have a data protection manager in organisations of more than 10 persons.
3. Questionnaires

3.1. Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA

3.1.1. Criterion 1 – Personal data involved

- Does the program/change require you to collect any personal data, such as detailed household consumption data, organisational measurement data, etc.?
- Will the personal data be combined with other data from outside the program/change?
- Can the data collected become personal due to linkage by third parties?
- Will the program/change require you to collect personal data from other systems?

3.1.2. Criterion 2 – Data controller/data processor

- Are you defining the conditions and the means of the processing operations (controller)?
- Are you conducting the processing on behalf of another organisation following their requirements (processor)?
- Have security and data protection requirements been defined between you and the processor/controller?

3.1.3. Criterion 3 - Impact on rights and freedom

- Are the privacy impacts on consumers unknown to your organisation?
- Do consumers have to give up control of their personal data?
- Are consumers able to control which data are collected? Are they able to control their data after it has been collected?
- Is it expected that consumers will change their behaviour due to the fact their personal data (e.g. energy consumption or change of supply) will be collected (freedom of choice might be jeopardized)?

3.1.4. Criterion 4 – When to perform a DPIA (right timing and motivation)

Are you:

- Designing a new program or service within the smart grid use case or situation?
- Making significant changes to an existing smart grid use case or situation?
- Operating a system in production without a DPIA having been carried out?
- Facing a data breach?
- Selecting a cloud based service for the processing operations using personal data?
3.1.5. Criterion 5 – The nature of the system/application exercise

**Purpose:**

- Is the purpose of collecting the personal data not clear or not shared with the consumers?
- Will the personal data collected by the program/change be used for any other purposes, including research and statistical purposes?
- Is the purpose of the program/change inconsistent with community values of privacy?
- Will the data be used for profiling?

**System:**

- Will the use of the technology or purpose from the program/change raise questions and/or resistance from the consumers?
- Are there new (e.g. unevaluated) measures being applied in the design of the technology?

**Organisational:**

- Are the roles and responsibilities for processing the personal data unclear?
- Will the personal data processing be executed by a third party processor?
- Will the personal data be transferred to other organisations?

3.1.6. Criterion 6 – Legal basis and public concern

- Is there a legal obligation to conduct a Data Privacy Impact Assessment?
- Is the legal basis for processing of consumer data still unidentified?
- Is there a legal framework for the application or the smart grid use case?
- Do you anticipate that the public will have any privacy concerns regarding the proposed program or change?

3.1.7. Other criterion

- Does the program/change contain any other measures that may affect privacy?

3.2. Step 2 - Initiation

<table>
<thead>
<tr>
<th>Aim of the DPIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;answer&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Team member name</th>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Inventory of necessary resources

<table>
<thead>
<tr>
<th>Interviewees</th>
<th>Documents</th>
<th>Other resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 3.3. Step 3 - Identification, characterization and description of Smart Grid systems/applications processing personal data.

#### 3.3.1. What is the detailed description of Smart Grid program/change according to M/490 Smart Grid Coordination Group use case template?

The support document can be found here:


<table>
<thead>
<tr>
<th>Domain</th>
<th>Name of Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Narrative of Use Case

- Short description – max 3 sentences

#### Complete description

#### Drawing or Diagram of Use Case “context diagram” and “sequence diagram” in UML

(as alternative, please include it in an annex and provide its name here)

<table>
<thead>
<tr>
<th>Scenario Name</th>
<th>Description of Information</th>
<th>Information</th>
<th>Information Exchanged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step No.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 3.3.2. What are the main scenarios of the Smart Grid use case?
3.3.3. Who are the main actors of the system?

<table>
<thead>
<tr>
<th>Actor Name</th>
<th>Actor Description</th>
<th>Individual (I) / Organisation (O) / System / Component (S)</th>
</tr>
</thead>
</table>

Table – Actors involved in the use case

The actors listed in the table above should be the ones involved in the personal data processing operations of the system/application which is under the scope of the DPIA.

3.3.4. How can the use case be mapped to a Smart Grid Business and ICT architecture (e.g. M/490 SGAM)?

At least the zones need to be identified in this reference architecture. The support document can be found in page 17 of the following file:

3.3.5. To which Smart Grid objective does the use case refer?

|-------|-----------|------------------|-----------|--------------------|-----------------|------------|----------|-------------------|------------------|

Table – Objectives of the use case
3.3.6. What are the primary and supporting assets of the smart grid?

Questions related to the primary assets:

- Which primary assets need to be protected?
- Which processing operation is concerned?
- What is its purpose?
- Who is it intended for?
- What business process is executed by this processing operation?
- Which data subjects are affected by this processing operation?
- How will the legal processes be implemented (i.e. right of access, rectification, etc...)?
- What kinds of personal data will undergo processing?
- What kinds of personal data will be used by the legal processes?

Questions related to the supporting assets:

- What supporting assets are used for the primary assets?
- Which kinds of hardware (computers, routers, electronic media, etc.)?
- Which kinds of software (operating systems, messaging systems, databases, business applications, etc.)?
- What are the kinds of computer communications networks (cables, Wi-Fi, fibre optics, etc.)?
- Who are the individuals involved?
- Which kinds of supporting paper assets (printouts, photocopies, etc.)?
- Which paper transmission channels (mail, workflow, etc.)?

3.4. Step 4 - Identification of relevant risks
### 3.4.1 Data Protection Threat identification

In order to facilitate the identification of threats, a non-exhaustive list of generic threats is provided below. They are grouped according to their impact on confidentiality, integrity and availability of the data.

#### 3.4.1.1 Threats that may jeopardize confidentiality

The following table presents the generic threats that can lead to:
- Illegitimate access to personal data,
- Compromise of processing (if this feared event is considered).

<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Abnormal use of hardware | Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.                                                                 | The use of uncontrolled hardware can introduce viruses in a normally clean environment. Energy companies which think they are secured against Internet threats become vulnerable from unexpected malware. 2nd: the use of hardware, which is not secure by energy companies, can cause serious risks (not able to mitigate DDoS attacks, the use of hard coded high privileged accounts with the use of simple username/password, not able to use VPN connections etc.). | 1. Are unknown devices accepted to use in the IT/OT environment?  
2. Are anti-virus and anti-malware measures present on all I/O-ports?  
3. Are crucial systems protected against the use of unknown storage devices (e.g. USB-devices)? | Reducing software vulnerabilities  
Reducing hardware vulnerabilities  
Reducing the vulnerabilities of computer communications networks |
| Hardware alteration  | Addition of incompatible hardware resulting in malfunctions; changing of components essential to the owner                                                                                                                                                                     | Changing of smart meter hardware can lead to changes of metering data which will damage the integrity of the consumption profile. This can affect the billing process and may cause reputation damage for the grid operator. | 1. Is change of hardware components present?  
2. Are measures in place to detect alteration in hardware in critical (smart energy) devices?  
3. Are these measures able to generate an alarm when a | Reducing hardware vulnerabilities |

<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Hardware espionage | Watching a person’s screen without them knowing while on the train; taking a photo of a screen; geo-location of hardware; remote detection of electromagnetic signals, shoulder-surfing etc. | Where copper wiring is still in use, it is possible to listen to the signals on the communication lines. This makes it possible to interpret and reuse signals send over the communications network. | 1. Includes an awareness program these topics replacing copper to fibre part of the planning?  
2. Are screen protectors in use to make it impossible to look at the screen or take pictures of the screen?  
3. Are measures taken to protect the data when using public wireless network?  
4. Are remote access controls disabled in an unprotected area (e.g. WiFi, Bluetooth, infrared)? | Reducing hardware vulnerabilities |
<p>| Hardware Key-logger | Hardware Key-logger logs all keystrokes. Allows attackers to reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc. | Hardware key-loggers can be used to collect data like usernames and passwords, commands, etc. This will make it possible to login the SCADA system and use a dispatcher’s role to communicate with the SCADA system. | 1. Are keyboard connectors, USB-ports and other I/O ports checked for unknown hardware devices on regular bases? | Reducing hardware vulnerabilities |</p>
<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Hardware loss              | Theft of a laptop from a hotel room; theft of a professional mobile phone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc. | Every device which contains sensitive data about the smart grid environment will cause unacceptable risk of alteration and abuse of those data. When information is retrieved about brand and type of firewalls, IP-ranges, OS and SCADA-system brand and type, a serious attack is made easy. | 1. Are hardware devices containing data protected against abuse? (password, Pin code, biometrical recognition, pattern recognition)  
2. Is the data in the hardware encrypted?                                                                                     | Reducing hardware vulnerabilities  
Reducing vulnerabilities related to the circulation of paper documents |
| Viewing of paper documents | Reading, photocopying, photographing, etc.                                                                                              | Paper documents with personal (metering, billing) information of the consumers are not securely stored and therefore accessible to unauthorized persons.                                               | 1. Are measures taken to prevent unauthorized access to paper documents with personal data?  
2. Is printing on demand installed?  
3. Are there secure lockers available to store printed data?                                                                         | Reducing the vulnerabilities of individuals  
Reducing the vulnerabilities of paper documents  
Reducing vulnerabilities related to the circulation of paper documents |
| Eavesdropping of computer channels | Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.                                             | Observation of metering and technical data between the smart meters and the central system with a false GSM base station by unauthorized person. | 1. Are measure taken to prevent interception? (like Man-in-the-middle-attack)  
2. Is time-stamping in place?  
3. Is authentication and authorisation in place to refuse unknown devices?  
4. Is the (wireless) connection between an authorized object                          | Reducing software vulnerabilities  
Reducing the vulnerabilities of computer communications networks |
| Remote espionage of individuals | Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings, etc. | Metering operators talking about personal information from consumers in their meetings or public areas. | 1. Are employees informed about security, security risks and vulnerabilities?  
2. Is awareness part of working meetings  
3. Are incidents shared to learn from them? | Reducing the vulnerabilities of individuals |
| Software Key-logger / Trojan Horse | Software Key-logger logs all keystrokes and/or Trojan sends commands and data to attacker's computer system | Allows attackers to engineer and reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc. | 1. Are all computer systems equipped with anti-virus, anti-malware solutions? (if available for the particular OS)  
2. Are anti-malware and anti-virus solutions updated on daily basis?  
3. Is anti-virus set so that the full computer scans on a regular basis? | Reducing software vulnerabilities |
### 3.4.1.2 Threats that may jeopardize integrity

The following table presents the generic threats that can lead to:
- Changes in processing,
- Unwanted changes of personal data,
- Alterations to legal processes (if this feared event is considered).

<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Software alteration           | Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc. | Changing smart meter software can lead to changes of metering data which will damage the integrity of the consumption profile. This can affect the billing process and may cause reputation damage for the grid operator. | 1. Is configuration management in place?  
2. Is patch management in place?  
3. Are software updates tested in a test environment, before use in the operational environment?  
4. Are source codes reviewed, when software is custom or customized for a specific system? | Reducing software vulnerabilities                                                   |
| Software function creep       | Content scanning; illegitimate cross-referencing of data; raising of privileges, wiping of usage tracks; sending of spam via an e-mail program; misuse of network functions, etc. | Meter operators have the privilege to make data accessible for viewing or manipulation (deletion, modification, movement, etc.). | 1. Is change of data authorized by a change management process?  
2. Are dedicated devices in use to change software function, to avoid unwanted introduction of viruses or malware? | Reducing software vulnerabilities                                                   |
| Man-in-the-middle attack via computer channels | *Man-in-the-middle attack* to modify or add data to network traffic; replay attack | A man-in-the-middle attack has been performed to modify the smart grid data so that the whole energy system will be unreliable. This may cause | 1. Is the data channel encrypted?  
2. Is time-stamping in place? | Reducing software vulnerabilities                                                   |
| Vulnerabilities of computer communications networks | Work overload | High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc. | When maintenance people are not skilled to do their job and/or stressed, there is high risk of unnoticed security breaches. They will recognize a security breach when systems are already going down, which is too late. | 1. Are employees adequately trained to do their job?  
2. Is the workload acceptable?  
3. Are employees trained to recognise vulnerabilities which can lead to a security breach? | Reducing the vulnerabilities of individuals |
|---|---|---|---|---|---|
| Forgery of paper documents | Changes to figures in a file; replacement of an original by a forgery, etc. | Changes to figures etc. is only possible in an environment where RBAC does not exist and people get much too much access rights. In a controlled environment where need to know and need to do is normal, this cannot be a problem. Falsifiable information can lead to unreliable consumer and metering information | 1. Are Identity and Access Management in place (e.g. Role Based Access Control)?  
2. For critical information change, is separation of duties in place? | Reducing the vulnerabilities of individuals |
| Insufficient access control procedures | Access rights are not revoked when they are no longer necessary. | (1) After a change of supplier the former supplier still has valid access credentials to (historic) read out meter data.  
(2) After moving house, the new tenant has access to historic readings in the meter.  
(3) Employees who change job positions are still authorized to access data, not necessary for their new job. | 1. Did you implement an access control policy?  
2. Who has access to the personal data?  
3. Does your access control policy cover all persons involved in processing personal data?  
4. How do you deal with access control rights when staff leaves the organisation?  
5. Do you have a regular review of the access control policy? | Managing persons within the organisation who have legitimate access  
Monitoring logical access controls  
Managing third parties with legitimate access to personal data |
<table>
<thead>
<tr>
<th>Issue Description</th>
<th>Details</th>
<th>Questions</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient information security controls</td>
<td>Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.</td>
<td>Load profile not end-to-end encrypted and could be read &amp; processed by unauthorized third party, e.g. a network provider.</td>
<td>1. Is an information security policy described, implemented and in place? 2. Have the information security controls been audited? Checked by an auditor?</td>
</tr>
<tr>
<td>Insufficient logging mechanism</td>
<td>The implemented logging mechanism is insufficient. It does not log administrative processes.</td>
<td>In a smart meter/ smart energy system it is not known which entity reads, collects, writes, changes or deletes data. After an incident, or just for routine checks, it is necessary to have logging information to abbreviate earlier activities.</td>
<td>1. What are the security controls taking non-repudiation into account? 2. How is the access to the personal data being logged?</td>
</tr>
<tr>
<td>Breach in security implementation</td>
<td>Though sufficient protective measures are theoretically in place, a breach in the implementation enables unauthorized parties to obtain access to personal data.</td>
<td>A faulty implementation of security mechanisms (locally or on a centralized server) enables hackers to access a memory area containing identifiable meter load profile history.</td>
<td>1. Did you perform a penetration test after implementation of the security controls? 2. How are the incident response management and the intrusion detection system implemented according to international standards?</td>
</tr>
</tbody>
</table>
| Access to data that was not intended (not necessary for the purpose of collection) | Unjustified data access after Change of Tenancy (CoT) or Change of Supply (CoS). | In case the tenant changes, the data from previous tenant is made available to the new tenant. In case of change of supply, old supplier still has access to data. | 1. Do you have procedures regarding personal data transfer after CoT or CoS? | Create procedures to address CoT and CoS.  
Active measure to preclude the use of particular data-items in the making of particular decisions.  
Destruction schedules for personal information. |
| The protection of data is compromised outside the European Economic Area (EEA). | There is a risk that smart metering data may be at risk if sent outside of the EEA. Another risk is that personal data like metering data gives inside information about vital infrastructures in an unknown, maybe untruthful environment. | Data protection standards outside the EEA may not be secure and robust as those countries are not subject to the obligations within the Data Protection Directive. Foreign organisations use information about vital infrastructures and personal information to investigate people of interest. | 1. Do you transfer the personal data outside the European Economic Area?  
2. To which country outside the European Economic Area is the personal data transferred to?  
3. Is the personal data transferred to a country that provides an adequate level of protection according to article 25 of Directive 95/46/EC?  
4. How did you guarantee the protection of the personal data when transferred outside the European Economic Area?  
5. Are all parties involved in implementation and operation established in the EU? | Anonymizing personal data  
Limiting personal data transfer to countries that provide an adequate level of protection according to the article 25 of the Directive 95/46/EC  
Active measures to preclude the disclosure of particular data-items  
Not transferring the source data, but only the outcomes |
| Inability to execute individual rights (inspection rights) | If data are going to be held by multiple data controllers, then consumers should have a means by which to access these data from multiple sources using a single subject access request. | Petrol station and organisation providing invoices work together to enable charging of vehicles in joint controllership. Individuals should be provided with easy means to get insight in the data collected (e.g. by a unified user access right). | 1. Is a procedure in place to easily inform consumers about the use of his personal data? | Informing data subjects  
Obtaining the consent of data subjects  
Giving the individual control over his data, for example by a secured website portal |
|---|---|---|---|---|
| Incomplete information | The information provided to the data subject on the purpose and use of data is not complete | Information provided to consumers only consists of usage data, information about other information (such as the ability to detect communication disruptions) gathered is not provided. | 1. How did you notify the purpose of the processing operation of personal data to the consumers? | Informing data subjects  
Clear and consistent communication of purpose and goals of data collection |
| Prevention of objections | Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible. | Consumers cannot opt out to reading of detailed energy load profiles because read-out schemes are not configurable: There are no technical or operational means to allow compliance with a data subject’s objection. | 1. Is it possible to change the collection of personal data in the smart grid use case after the consumer’s objection?  
2. Can consumers object to processing of personal data use by certain technologies? | Permitting the exercise of the right to object  
Make a privacy policy, code of conduct or certify the processing of the data to be more transparent |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Questions</th>
<th>Context</th>
</tr>
</thead>
</table>
| Unclear responsibilities for data processing.                        | It is not clear to data subjects what parties are involved in the processing of data and their respective roles.                                                                                               | 1. Are responsibilities clearly described and carried out for all parties?  
2. Is responsibility for data processing part of a subcontractors contract? | Informing data subjects                                                                                                                                                                                  |
|                                                                      | (1) Installation organisation is acting as a subcontractor for the metering operator and is collecting data for the grid operator.  
(2) The energy service company (ESCo) hires a third party to collect data to provide energy saving advice to the consumer. |                                                                                                                                                                                                          | Make a privacy policy, code of conduct or certify the processing of the data to be more transparent |
| A lack of transparency for automated individual decisions             | Automated processing of personal data intended to evaluate certain personal aspects or conduct is used but the data subjects are not informed about the logic of the decision-making. | 1. Are consumers informed of automated information processing?  
2. How are the consumers notified of automated individual decisions? | Informing data subjects                                                                                                                                                                                  |
|                                                                      | Remote disconnect is performed without clear explanation provided to the user or the reasons why.                                                                                                           |                                                                                                                                                                                                          |                                                                                                                                 |
| Lack of quality of data for the purpose of use                        | If data is used for certain processes it should be adequate.                                                                                                                                                 | 1. Are automated input validation and reconciliation controls implemented?  
2. How do you ensure data quality for the purpose of use?  
3. Are there test procedures for data quality? | Monitoring the integrity of personal data                                                                                                                                                                  |
|                                                                      | For billing on a daily basis data should be registered on a daily basis. For disconnecting electricity supply the exact location (address) and reasons should be conclusive. Based upon wrong consumption data a wrong invoice is sent. A comma is used as a separator where a full-stop is intended. This leads to wrong invoice. |                                                                                                                                                                                                          | Introduction of automated controls on the data quality                |
| Lack of access to personal data | There is no way for the data subject to initiate a correction or erasure of his data. The data controller and/or processor are not sufficiently prepared to respond to such requests. | A personalized overview of personal data cannot be generated from the database that holds the data. | 1. Are there processes to meet the consumer’s rights on data collection, access, deletion and correction?  
2. Are you able to provide overview of data collected?  
3. Are you able to provide what data is transferred to a third party?  
4. Can an overview of what data is provided to whom be provided?  
5. Are you able to delete the data on request? | Permitting the exercise of the direct access right  
Allowing the exercise of the right to correct  
Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers  
Give the individual control over his data, for example by a secured website portal |
| Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner. | The data is distributed across several business units and an integrated overview cannot be made within a short time frame. | Metering data is stored and maintained by the technical department, reactions on commercial offers are stored at the commercial department, questions and answers are stored at the service department. Combining this data in one overview takes (a lot of) effort. | 1. Are there processes to meet the consumer’s rights on data collection, access, deletion and correction? 2. Are you able to provide overview of data collected? 3. Are you able to provide what data is transferred to a third party? 4. Can an overview of what data is provided to whom be provided? 5. Are you able to delete the data on request? | Allowing the exercise of the right to correct Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers Give the individual control over his data, for example by a secured website portal |
| Abnormal use of software | Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc. | Unauthorized changes of personal data, metering data, etc. make the system unreliable. | 1. Is access control in place? 2. Is the authorization structure well-tuned? 3. Are authorizations checked on a regular basis? 4. Are authorizations revoked immediately after job change or dismissal? 5. Are system operations logged? 6. Is separation of duties in place in critical system operations? | Reducing software vulnerabilities |
3.4.1.3 Threats that may jeopardize availability

The following table presents the generic threats that can lead to:

- Unavailability of legal processes,
- Disappearance of personal data,
- Unavailability of processing (if this feared event is considered).

<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware loss</td>
<td>Theft of a laptop from a hotel room; theft of a professional mobile phone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc.</td>
<td>Every device which contains sensitive data about the smart grid environment will cause unacceptable risk of alteration and abuse of those data. When information is retrieved about brand and type of firewalls, IP-ranges, OS and SCADA-system brand and type, a serious attack is made easy.</td>
<td>1. Are hardware devices containing data protected against abuse? (password, Pin code, biometrical recognition, pattern recognition) 2. Is the data in the hardware encrypted?</td>
<td>Reducing hardware vulnerabilities  Reducing vulnerabilities related to the circulation of paper documents</td>
</tr>
<tr>
<td>Loss of Power</td>
<td>Loss of power can harm hardware and software and lead to unavailability of computing systems, network equipment and disruption of smart grid devices</td>
<td>Examples: Due to power loss crash of hard drives or other hardware components; Due to power loss crash of OS or loss of unsaved data; Long time power loss has impact on availability of systems. Not all systems will be covered by emergency power equipment; Very long time loss of power will lead to disruption in refuelling emergency power and lack of emergency power.</td>
<td>1. Are measures taken to avoid disruption of power, such as UPS and no-break? 2. For vital information systems are uninterruptible power supplies in place? 3. Are there provisions made in order to refuel in time?</td>
<td>Reducing software vulnerabilities  Reducing hardware vulnerabilities  Reducing the vulnerabilities of computer communications networks</td>
</tr>
</tbody>
</table>
| Denial of service | Denial of service will lead to unavailability of computing systems | DDoS attacks can lead to unavailability. Consumers cannot reach websites of supplier. Smart grid components cannot communicate, which leads to disruption of the self-healing opportunities of the grid. | 1. Are attack scenarios investigated and known?  
2. Are mitigating measures in place to detect and stop a DDoS attack?  
3. Is a Disaster Recovery plan in place to recover as soon as possible after a successful attack? | Reducing hardware vulnerabilities  
Reducing the vulnerabilities of computer communications networks |
3.4.1.4 Threats that may jeopardize personal data

The following table presents the generic threats that can lead to:

- Breaches of legal processes,
- Breach of use of personal data

<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Collection exceeding purpose         | More personal data is collected than what is necessary to achieve a specified purpose. | Collecting more detailed load profile data for the purpose of monthly billing, where much less detailed data would be sufficient to achieve the same objective. | 1. What personal data do you need to collect for the purpose?  
2. Is the collected data proportional to the purpose? | Minimizing the amount of personal data  
Active measure to preclude the use of particular data-items in the making of particular decisions  
Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application for any other purpose |
<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Combination exceeding purpose       | Personal data is combined to an extent that is not necessary to fulfil the specified purpose. | Information in smart metering load profile used for billing is combined with personal data obtained from a third party to provide (third party) additional targeted services or products (e.g. insurance for stability in energy supply) | 1. Will the personal data be combined with other data outside the scope of the system/application?  
2. Is the personal data only collected for that specified predetermined purpose? | Minimizing the amount of personal data  
Active measure to preclude the use of particular data-items in the making of particular decisions  
Active measures to preclude the disclosure of particular data-items  
Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose |
<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Missing erasure policies or mechanisms; excessive retention periods            | Data is retained longer than necessary to fulfil the specified purpose or to comply with legal obligations. Detailed metering data is kept in a database for longer than necessary to achieve its purpose and/or longer than required by law, for example, because of the absence of automatic deletion of obsolete data or because excessive retention periods have been established, without due regard to data protections requirements. | Metering data in energy systems is retained for x period in line with generic Archive Laws but is should only be retained in line with data retention policy, because it is not needed for the purpose anymore.                                                                                                                                                                                                                                                                  | 1. Is there a legal obligation defining the data retention period?  
2. Do you have data retention policy implemented?  
3. What is the retention time of the personal data?  
4. What are the measures to delete the personal data after this retention time?  
5. Is there an auditing mechanism to inspect the erasure policies or mechanisms?  
6. Is it necessary to store the data for this retention period considering the purpose?                                                                                                                                                                                                           | Managing personal data retention periods  
Active measure to preclude the use of particular data-items in the making of particular decisions  
Minimisation of personal data retention by destroying it as soon as the transaction for which it is needed is completed  
Destruction schedules for personal information                                                                                                                                                                                                                                                   |
<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undeclared data collection</td>
<td>Some data is secretly recorded and thus unknown to the data subject.</td>
<td>The DSO does remote meter readings of detailed load profile without consumer's awareness.</td>
<td>1. Are consumers informed about collection of personal data, timing, data retention, usage</td>
<td>Informing data subjects</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Is any data collected without consumer notification?</td>
<td>Clear and consistent communication of purpose and goals of data collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Are you collecting any data without informing the consumer?</td>
<td></td>
</tr>
<tr>
<td>unlimited purpose</td>
<td>Personal data is used for additional purposes that have not been adequately justified and documented to the data subject.</td>
<td>In an energy system metering billing information can also be used for marketing goals and awareness about energy consumption and CO₂ emissions and for selling targeted electricity schemes.</td>
<td>1. What is the purpose of using the personal data?</td>
<td>Informing data subjects</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Is the purpose S.M.A.R.T. defined?</td>
<td>Clear and consistent communication of purpose and goals of data collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Are all purposes of use in line with purpose of collection?</td>
<td></td>
</tr>
<tr>
<td>Generic threats</td>
<td>Explanation of threats</td>
<td>Specific Energy industry examples of supporting asset vulnerabilities</td>
<td>Questions for guidance</td>
<td>Controls (example)</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Invalidation of explicit consent | When consent is used as a legal basis for data processing, it must be: (a) freely given (b) specific and (c) informed indication of the user’s wishes. If any of these conditions are not met, consent is invalid. | (1) Consumer is only offered significantly higher tariffs unless he accepts the use of his load profile data for marketing purposes (in this case the consent is not freely given); (2) consumer is not informed of the possibility that his load profile data may be disclosed to third parties for marketing purposes when requested to opt in to half-hourly readings (consent is not given on informed base); (3) consumer is required to give consent to detailed (e.g. half-hourly) meter readings even when he does not wish to sign up for a time-of-use tariff; (4) consumer provides consent based upon general contract conditions (implicit consent instead of explicit); (5) The consumers accepts an electricity scheme without signature. | 1. How did you ask and receive the explicit consent from the consumer? 2. What were the choices for the consumers (for system, type of data, and way of collecting)? 3. What are the consequences for the consumer if his consent is not given? | Informing data subjects  
Obtaining data subjects' consent  
Non-collection of contentious data-items  
Non-collection of identifiable information, only pseudonyms, or anonym data  
Use of mathematical methods without collecting and registration source data to reach goals  
Clear and consistent communication of purpose and goals of data collection |
<table>
<thead>
<tr>
<th>Generic threats</th>
<th>Explanation of threats</th>
<th>Specific Energy industry examples of supporting asset vulnerabilities</th>
<th>Questions for guidance</th>
<th>Controls (example)</th>
</tr>
</thead>
</table>
| Non legally based personal data processing          | Processing of personal data is not based on consent, a contract, legal obligation, or other relevant legal ground as per Article 7 of Directive 95/46/EC.                                                                               | (1) A smart grid operator shares collected information with a third party without notice, consent or as otherwise legally allowed. (2) New parties connect to the grid and use information for purposes not specified in the electricity law, although highly related (e.g. petrol stations connect for the purpose of charging vehicles but also need to maintain stability in energy supply). | 1. Is the collection of personal data based on explicit consent and/or legitimate grounds?  
2. What is the legitimate ground for collection the personal data?                     | Obtaining the consent of data subjects  
Minimizing the amount of personal data  
Make a privacy policy, code of conduct or certify the processing of the data to be more transparent |
| Lack of transparency                                 | Data processing is not made transparent, or information is not provided in a timely manner.                                                                                                                             | Information available to consumers that lacks clear information on how data is processed and used, the identity of the Operator, or the user’s rights.       | 1. Are consumers informed about type of data, data retention policy, transfer of data to third parties?  
2. Do you notify the consumers about their privacy and data protection rights? | Informing data subjects  
Make a privacy policy, code of conduct or certify the processing of the data to be more transparent |
3.4.1. Data Protection Threat identification - Outcome of the questionnaire

Within the table below the selection made from the table in section 3.4.1 of identified threats should be listed. A feared event should be associated with one or more threats.

<table>
<thead>
<tr>
<th>Feared events</th>
<th>Threat ID</th>
<th>Threat name</th>
<th>Brief explanation why relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feared event 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..............</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feared event 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..............</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feared event 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..............</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 3.5. Step 5 - Data Protection Risk Assessment

<table>
<thead>
<tr>
<th>Level of identification + prejudicial effects</th>
<th>Severity/impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 5</td>
<td>1. Negligible</td>
</tr>
<tr>
<td>= 5</td>
<td>2. Limited</td>
</tr>
<tr>
<td>= 6</td>
<td>3. Significant</td>
</tr>
<tr>
<td>&gt; 6</td>
<td>4. Maximum</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting asset vulnerabilities + risk source capabilities</th>
<th>likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 5</td>
<td>1. Negligible</td>
</tr>
<tr>
<td>= 5</td>
<td>2. Limited</td>
</tr>
<tr>
<td>= 6</td>
<td>3. Significant</td>
</tr>
<tr>
<td>&gt; 6</td>
<td>4. Maximum</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feared events</th>
<th>Threat ID</th>
<th>Related Privacy targets</th>
<th>Affected assets</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feared event 1</td>
<td>..........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feared event 2</td>
<td>..........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feared event 3</td>
<td>..........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Map for locating the feared events from their risk level **without** considering the controls (source CNIL):

<table>
<thead>
<tr>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Maximum</td>
<td>1. Negligible</td>
</tr>
<tr>
<td>3. Significant</td>
<td>2. Limited</td>
</tr>
<tr>
<td>2. Limited</td>
<td></td>
</tr>
<tr>
<td>1. Negligible</td>
<td></td>
</tr>
</tbody>
</table>

### 3.6. Step 6 – Identification and Recommendation of controls and residual risks

#### Control identification table and residual risks

<table>
<thead>
<tr>
<th>Feared events</th>
<th>Threat ID</th>
<th>Controls planned or implemented</th>
<th>Risk level</th>
<th>Risk treatment (including implementation of privacy targets)</th>
<th>Residual risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feared event 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feared event 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feared event 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Map of feared events **with** implemented or planned controls:

#### Severity

- **1. Negligible**
  - Feared event 1
  - Feared event 3
- **2. Limited**
  - Feared event 1
- **3. Significant**
  - Feared event 2
- **4. Maximum**
  - Feared event 4
**Article 29 Working Party**
The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

**CSO**
Charge Spot Operator

**CSP**
Charge Service Provider

**CoS**
Change of Supply

**CoT**
Change of Tenancy

**Data Controllers**
Data Controllers observe a number of principles when they process personal data. These principles not only protect the rights of those about whom the data is collected ("data subjects") but also reflect good business practices that contribute to reliable and efficient data processing.

**Data Subject**
An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

**DG**
Distributed Generation

**DPA**
Data Protection Authority - supervises the compliance with acts that regulate the use of personal data.

**DPIA**
Data Protection Impact Assessment

**DPO**
Data Protection Officer - The main task of the DPO is to ensure, in an independent manner, the internal application of the provisions of the Regulation in his/her organisation.

**DSO**
Distribution System Operator - A distribution system’s network carries electricity from the transmission system and delivers it to consumers.

**EC**
European Commission

**EEA**
European Economic Area

**EV**
Electric Vehicle
Grid Operator: Transmission (TSO) and distribution system/network operators (DSOs).

Information Security: Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.


IT: Information Technology

M490 Standardisation mandate: Standardization Mandate to European Standardization Organisations (ESOs) to support European Smart Grid deployment.

Personal Data: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Privacy: Defined as the right to be left alone and includes elements of protecting private life such as integrity of a person’s home, body, conversations, data, honour and reputation following the Article 7 of the Charter of fundamental rights of the European Union.

Residual Risks: The remaining risk after the treatment of a risk

Risk Assessment: Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard)

SG-SC: Smart Grid Coordination Group

SGTF: Smart Grid Task Force

SMART: Systems Management of Alert Responsive Tasks' - is a mnemonic to guide people when they set objectives, often called Key Performance Indicators (KPIs), for example for project management, employee performance management and personal development.

Smart Grid: An electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety”.

SME: Small and Medium Enterprises
**SRO**
Senior Risk Owner - is an Executive Director or Senior Management Board Member who will take overall ownership of the Organisation’s Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation’s Statement of Internal Control in regard to information risk.

**WG RA**
Workgroup on Reference Architectures

**WG SGIS**
Workgroup on Smart Grid Information Security

**ANNEXES**

**Annex I – Privacy and data protection targets**
Embedded in Directive 95/46/EC and reflecting on-going EU regulatory developments and practices, this list of privacy targets and the associated risks of smart grid applications constitute the core element of the development of the DPIA Process. While all targets are essential elements of organisational compliance, in many cases only a subset of these requirements will be at issue in the application under consideration.

<table>
<thead>
<tr>
<th>Description of privacy targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguarding quality of personal data</td>
</tr>
<tr>
<td>Legitimacy of processing personal data</td>
</tr>
<tr>
<td>Legitimacy of processing sensitive personal data</td>
</tr>
<tr>
<td>Compliance with the data subject’s right to be informed</td>
</tr>
<tr>
<td>Compliance with the data subject’s right of access to data, correct and</td>
</tr>
<tr>
<td><strong>erase data</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>Compliance with the data subject’s right to object</strong></td>
</tr>
<tr>
<td><strong>Safeguarding confidentiality and security of processing</strong></td>
</tr>
<tr>
<td><strong>Compliance with notification requirements</strong></td>
</tr>
<tr>
<td><strong>Compliance with data retention requirements</strong></td>
</tr>
<tr>
<td><strong>Privacy by design</strong></td>
</tr>
<tr>
<td><strong>Privacy by default</strong></td>
</tr>
</tbody>
</table>
Annex II – List of possible controls

Minimizing the amount of personal data

Objective: to reduce the severity of risks by limiting the amount of personal data to what is strictly necessary to achieve a defined purpose.

Managing personal data retention periods

Objective: to reduce the severity of risks by ensuring that personal data is not retained for longer than necessary.

Informing data subjects

Objective: to ensure that the subjects are informed.

Obtaining the consent of data subjects

Objective: to allow data subjects to make a free, specific and informed choice.

Managing persons within the organisation who have legitimate access

Objective: to reduce the risks associated with persons within the organisation (employees, seconded subcontractors, interns and visitors) who have legitimate access to personal data.

Managing third parties with legitimate access to personal data

Objective: to reduce the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.

Monitoring logical access controls

Objective: to limit the risks that unauthorized persons will access personal data electronically.

Partitioning personal data

Objective: to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.

Encrypting personal data

Objective: to make personal data unintelligible to anyone without access authorization.

Anonymizing personal data

Objective: to remove identifying characteristics from personal data.

Protecting personal data archives

Objective: to define all procedures for preserving and managing the electronic archives containing the personal data.
Managing personal data violations

*Objective:* to have an operational organisation that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.

Tracing the activity on the IT system

*Objective:* to allow early detection of incidents involving personal data and to have information that can be used to analyse them or provide proof in connection with investigations.

Combating malicious codes

*Objective:* to protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of personal data.

Reducing software vulnerabilities

*Objective:* to reduce the possibility to exploit software properties (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.) to adversely affect personal data.

Reducing hardware vulnerabilities

*Objective:* to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

Reducing the vulnerabilities of computer communications networks

*Objective:* to reduce the possibility to exploit communications networks properties (wired networks, Wi-Fi, radio waves, fibre optics, etc.) to adversely affect personal data.

Reducing the vulnerabilities of paper documents

*Objective:* to reduce the possibility to exploit paper documents properties to adversely affect personal data.

Reducing vulnerabilities related to the circulation of paper documents

*Objective:* to reduce the possibility to exploit paper document circulation properties (within an organisation, delivery by vehicle, mail delivery, etc.) to adversely affect personal data.

Create procedures to address CoT and CoS

*Objective:* To ensure that after such a change, no personal data is available

Permitting the exercise of the right to object

*Objective:* to ensure that individuals have the opportunity to object to the use of their personal data.

Monitoring the integrity of personal data

*Objective:* to be warned in the event of an unwanted modification or disappearance of personal data.
Allowing the exercise of the right to correct

Objective: to ensure that individuals may correct, add, update, block or delete their personal data.

Permitting the exercise of the direct access right

Objective: to ensure that individuals have an opportunity to know about their personal data.

Reducing the vulnerabilities of individuals

Objective: to reduce the possibility to exploit people (employees, individuals who are not part of an organisation but are under its responsibility, etc.) by adversely affecting personal data.

Non-collection of contentious data-items

Objective: to avoid collection of data-items against client’s wishes.

No collection of identifiable information, only pseudonyms, or anonym data

Objective: to prevent identification of the data subject through collected data.

Purpose limitation, e.g. taking appropriate measures to ensure that personal data is only used for the purposes defined beforehand and not used for other related or unrelated purposes

Objective: to ensure that personal data is only used for the purposes defined beforehand and not used for other related or unrelated purposes.

Active measure to preclude the use of particular data-items in the making of particular decisions

Objective: to ensure that decisions are made based only on due data-items.

Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose

Objective: to ensure that information is used for the specified purpose and for nothing more than that.

Active measures to preclude the disclosure of particular data-items

Objective: to ensure that only required and permitted data-items are disclosed.

Minimisation of personal data retention by destroying it as soon as the transaction for which it is needed is completed

Objective: to ensure compliance with legislation and to prevent misuse of personal data.

Destruction schedules for personal information

Objective: to ensure compliance with legislation and to prevent misuse of personal data.

Use of mathematical methods without collecting and registration source data to reach goals

Objective: to avoid collection of non-authorized data without prejudice to reach goals.
Clear and consistent communication of purpose and goals of data collection

*Objective:* to ensure that the client and other interested parties are clearly informed of purpose and goals of data collection.

Make a privacy policy, code of conduct or certify the processing of the data to be more transparent

*Objective:* to establish rights, responsibilities and boundaries in order to make data processing transparent to those involved.

Not transferring the source data, but only the outcomes

*Objective:* to avoid disclosure of undue data.

Give the individual control over his data, for example by a secured website portal

*Objective:* to ensure that the individual has control over his data according to his rights and responsibilities.

Introduction automated controls on the data quality

*Objective:* to ensure that data quality is monitored and maintained on a regular basis.

Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers

*Objective:* to ensure that clients have a way of communicating their requests and complaints and to ensure that these are timely and adequately addressed.

Audit

*Objective:* this is a generic control to ensure that all implemented controls are in place.
Bibliography

