05 December 2011

Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection

Recommendation to the European Commission

Version 1.0

Acknowledgements

The following European organizations were involved in the creation of this report and acknowledge its content:

BEUC	DIGITAL EUROPE	ETSI
CEDEC	EDSO / DSO Club	EURELECTRIC
CEER	ESIA	GEODE
CEN/CENELEC	ESMIG	T&D EUROPE

Executive summary

This report contains the recommendations by the Expert Group 2 (EG2) that were drafted between 30 November 2010 and 31 March 2011. The report was amended after public consultation on 6 May 2011. The recommendations aim to provide guidance on the essential regulatory requirements for data handling, data safety and consumer protection in Smart Grids.

The recommendations are the result of a joint effort by the EG2 members. These recommendations are considered essential in the sense that they provide a fundamental basis for regulatory action that is to be taken. They stem from the principles that are laid out in the legal bases within the legislative structures in the European Union and – where appropriate – the individual Member States. We stress that although European legislation takes precedence over national legislation, national structures should be taken into account when these recommendations are considered to be effectuated.

In conjunction with these recommendations we want to stress the need for consideration of the (financial and technological) steps that have currently been taken by the different actors involved in Smart Grids, without diminishing the importance of sound guidance on this topic. It is important to be mindful of both the need for consumer protection and the importance of the freedom to innovate to achieve social and economic welfare. The technological solutions mentioned in this report should not all be viewed as requirements in this light, unless stated otherwise. They can be seen as suggested solutions for the specific issues at hand.

The basis for the recommendations is given in the main text of the report. The report consists of a description of current legal and regulatory privacy aspects, privacy in Smart Grids, Security in Smart Grids and measuring instruments. The recommendations are following their nature classified in general, privacy, security and telecom related clusters.

During the drafting of the report a number of relevant topics were discussed. These topics are not within the scope of the EG2, but have been added to the report as appendices. These appendices do not contain recommendations by the Expert Group, but provide support and background for the statements in the report.

Summary of recommendations

General

EG2.#	Recommendation
EG2.G.1	The European Smart Grid regulation should utilise and implement decision 768/2008/EC as it will need to be harmonised to products already harmonised under NLF. This should be the case for all products that will be interchangeably integrated and that should seamlessly interoperate as actor in the Smart Grid with other system components of the Grid.
EG2.G.2	Following a clarification of the relationship between the standards produced by the ESOs under the standardisation mandate and future legislative initiatives at the European level, the Standards need to be developed by standardisation organisations based on a common set of use-cases taking into account the different business models across the Member States. The standardisation organisations will maintain these standards over time as Smart Grid applications evolve.

EG2.G.3	Enforcement is a key aspect of regulation. There are many relevant authorities within the European Union at the different organisational levels. In order to be able to effectively enforce regulation guidelines need to be developed on monitoring and enforcement. It is recommended to address the Member States to review their regulatory frameworks in order to be able to enforce the use of common standards across the European Union.

Privacy and data protection

EG2.#	Recommendation
EG2.P.1	The introduction of Smart Grids with intelligent meters changes the polling frequency of measurement and the coverage of the measurement at the consumer location. Whereas up to now the frequency is low and covers an area or larger number of energy users, the intelligent meter may revolutionise the frequency to minutes or real-time whereas the coverage is in the order of individual consumers or households. This implies that where up to now the operator has a broad view of the energy behaviour of a larger set of consumers, this view will evolve to detailed information on the energy behaviour of sole end consumers. Because of this shift in detail it is recommended to confirm that in accordance with opinion 183 of the Article 29 Data Protection Working Party most data from Smart Meters can be considered personal data and to determine the extent to which the various data at different levels of detail can be considered as such.
EG2.P.2	The implementation of Smart Grids potentially connects location information to specific data that holds information on the use of electrical energy, and in the future possibly more. The fingerprint or contents of this data provides information on what is going on at the location at a specific moment, and may show patterns over longer time which may have great impact on the privacy and security of the consumer. It is recommended that adequate measures are deployed to protect the contents and nature of this data in order to safeguard the privacy of the consumer.
EG2.P.3	Privacy by Design and by Default should be strongly encouraged and can be incorporated in the methodologies of parties involved in Smart Grid development when personal data are involved. The application of this principle can effectively incorporate privacy measures into the development process and can improve control over the processing for the consumer.
EG2.P.4	Member States to Member States to Error! Not a valid bookmark self-reference.
EG2.P.5	Given the variety of data storage purposes within smart metering, a single data retention period cannot be concluded. In other words, each such purpose has its own characteristics and a specific data retention period. Next, we cannot interfere with national criminal (tax) laws and civil procedures.
EG2.P.6	EG2 recommends Member States to perform an analysis in order to determine to which extent utilities need to retain personal data (i.e. neither non-aggregated nor anonymised) to be able to maintain and operate the electrical grid and perform billing.
EG2.P.7	Following EG2.P.6, the following principles should apply for the purpose of data retention: (a) data minimisation – i.e. the scope and length of both (i) data collection and (ii) data retention shall in any case not exceed what is necessary to achieve specific and lawful purpose. (b) transparency – i.e. who, when and in what circumstances collects, processes and retains personal data for what purposes, and what data and where is stored; (c) empowerment of the consumer – i.e. safeguarding consumer's rights (including information). In case the personal data are to be collected and processed – to ensure full compliance with the data protection Directive, namely the principles of data minimisation (Art. 6(b)-(c) of the 1995 Data Protection Directive). A recommendation on specific retention periods is shown in section 2.2.2.6.
EG2.P.8	The use of privacy certification schemes should be encouraged by Member States. When provided by independent parties these schemes can provide transparency and trust to customers as well as for the actors responsible for the Smart Grid. Further research to

	determine which certification scheme, strict criteria and structure should be used is necessary.
EG2.P.9	The opinions on the protection of personal data from Smart Grids differ widely between Data Protection Authorities (DPAs). In order to be able to adequately protect consumer rights and enable the effective use of Smart Grids DPAs need to be involved in the process, but also need to be able to apply a consistent set of responsibilities, definitions and principles. DPAs should be involved in these steps, but the actors should be able to show accountability themselves. Accountability should enhance not replace the obligations of the data controllers to comply with data protection legislation.
EG2.P.10	Privacy is a constitutional standard in contemporary European democracies. Non-compliance with privacy limitation criteria might have an adverse effect on Smart Grids deployment in a given electricity market. It is recommended that both a regulatory framework is enacted and a practice that respects these limitation criteria is introduced. We recommend that interference should be justified on a case-to-case basis, assessing legality, necessity, legitimacy, proportionality.
EG2.P.11	It is recommended that specific measures are taken to ensure the adequate protection of personal data in smart metering. The fact that smart metering may be necessary for the society as a whole should not suffice to override the fundamental right to protection of privacy. Any solution must comply with the law on data protection and privacy. This position has also been supported by the opinion of Article 29 Data Protection Working Party. The fact that smart metering may be necessary for the society as a whole should not suffice to override the fundamental right to protection of privacy. Any solution must comply with the law on data protection and privacy. This position has also been supported by the opinion of Article 29 Data Protection Working Party.

Security

EG2.#	**Recommendation**
EG2.S.1	An important task for the European Commission is the creation of a trusted network of public and private organisations, where information about incidents, threats, vulnerabilities and good practices will be shared intensively. Point of departure is that companies themselves will only take effective measures if they have access to the right information and are able to make accurate risk assessments. The participants can prevent incidents themselves. This will safeguard the European economy as a whole and the continuity of the individual organisations at the same time. ENISA can play an important role in facilitating this Information Exchange within the electricity sector, but also with governments, IT & Telecom providers, vendors & integrators, academia and research institutions. Existing information exchanges like the EuroSCSIE (European SCADA and Control Systems Information Exchange) can form a good basis for this.
EG2.S.2	Energy supply core functionality requirements should include: uninterrupted service (subject to allowable disconnection and prepayment usage), black start capability and little dependencies on other critical infrastructures. Also, all functionalities need to be robust and resilient. Furthermore, the less critical processes on energy supply should not endanger the more critical ones. Processes should be able to handle disruptions and return to normal operations afterwards. These requirements should be fulfilled even in case of breakdown, failure or targeted attacks to the ICT architecture of the Smart Grids. The impact of ICT problems on energy delivery should be kept as low as possible. Regarding smart metering this would mean that failures within parts of the smart metering infrastructure including the used ICT-networks must not lead to blackouts or impair other processes more critical for electricity delivery more than unavoidable. ESOs to ensure principles are reflected in standards.
EG2.S.3	The European Commission should play an important role in creating awareness of the importance of security while implementing Smart Grids. This should be done on all levels, but the EC can play especially have an important influence at the CEO-level in the electricity industry, but also cross-sectoral in the telecommunications industry. It would be a good idea introducing this strategic level at a Ministerial top conference on the security and privacy of

	Smart Grids, with the aim of producing a joint public-private roadmap to secure Smart Grids.
EG2.S.4	A trusted smart meter infrastructure will eventually very likely be based on certificates being released by certification authorities. It is recommended that national certification authorities are involved in Smart Grids prior to a roll-out of devices. These national authorities (similar to or even included in Data Protection Authorities) can operate a national trust centre. It is recommended to make sure the implementation of these certification authorities and trust centres is done at the Member State level, although alignment within the EU is important to prevent difficulties for internationally operating actors and guarantee a level playing field. High investments needed for certification of devices may hinder their introduction.
EG2.S.5	Within a trusted network of public and private organisations the European Commission can promote and facilitate: the development of security guidelines for Smart Grids, keeping existing guidelines like the NISTIR-7628 in mind; the certification of products and services (similar like the Certification Program that was built for the Process Control Domain Security Requirements for Vendors from the WIB); test facilities, where new architectures and it's components can be tested; Research & Development in the area of the security and privacy of Smart Grids. A periodic check on adequacy of measures taken (such as the International Security Forum's health check) can aid in the awareness of the current effectiveness.
EG2.S.6	The level of experience and awareness can be increased within a trusted network of public and private organisations by providing (online) training and information facilities.

Measuring Instruments

EG2.#	Recommendation
EG2.M.1	1 Because logical components of Smart Grids may be incorporated in different physical devices the guidelines should focus on requirements for the logical infrastructure. MID relevant devices like smart meters will play an important role in a real infrastructure but their architecture is currently focused on MID or national conformity only. The Measuring Instruments Directive 2004/22/EC (19) provides the necessary requirements for smart meters and other measurement components. The Measuring Instruments Directive 2004/22/EC (19) provides the necessary requirements for smart meters and other measurement components.
EG2.M.2	The European Smart Meter Requirements (ESMR) provide a good basis for technical requirements for meters and other Smart Grid components. It is recommended to further develop the ESMR in order to set up a technical standard for Smart Metering devices, and to consider introducing similar requirements for Smart Grids.

Table of contents

Introductory comments

Smart Grids are the amongst the most promising future developments to manage and control our energy consumption in the next decades and they are believed to be going to re-shape the electricity power grid. However, the integration and interdependencies that will evolve between the electricity power grid, telecommunication networks and ICT are a permanent cause for concern. New threats and vulnerabilities introduced to this critical infrastructure must be recognised and understood. It is believed that Smart Grid security and privacy issues can be addressed adequately with the right kind of security controls, balanced risk mitigation strategies and a continuous attention towards security, privacy and regulation aspects on both strategic and operational levels.

This report contains the findings of the Smart Grids Task Force Expert Group 2 of the Directorate-General Energy addressed to the European Commission on the *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection*. Contained in this report are the following subjects, divided in the appropriate chapters:

- A general approach on privacy legislation and regulation within the European Union.
- An application of the general approach to the specific case of Smart Grids
- Security recommendations that are applicable to Smart Grids.
- Recommendations that follow from measuring legislation and regulation.

In the various appendices of the report background information is given that may be of relevance to the reader and can provide elaboration on subjects that are influenced by Smart Grids. In addition, the subject of Smart Grids and its applications may need some further introduction. This introduction is given in appendix A.

The relevant recommendations as shown in the executive summary are within the scope of EG2 and are all contained (with their respective motivation) in the main section.

1. Legislation, Regulation, Standardisation and Enforcement

1.1. Privacy and data protection in the EU

1.1.1. Definitions

01 There is a difference between the right to privacy and the right to protection of personal data. The distinction made in the EU Charter on Fundamental Rights (CFR) (1) is followed here.

02 Privacy is usually defined as the ability of an individual to be left alone, out of public view, free from surveillance or interference from others (individuals, organisations or the state) and in control of information about himself (2). The idea of privacy originates from the famous article by Samuel Warren and Louis Brandeis titled '*The Right to Privacy*' (1890) (3). A number of legal definitions can be found in the respective instruments, e.g. Article 8 of the European Convention on Human Rights (ECHR)[1].

03 The ability to prevent intrusion into the physical space of a subject ('physical privacy') and the ability to control the processing of data of a subject ('informational privacy') are separate concepts. Privacy overlaps but does not coincide with data protection. The right to protection of personal data protects all personal data, even when there is no strong link with privacy, whereas the right to privacy, in the view of the European Court on Human Rights (ECtHR), only protects personal data in cases where the Court finds a link with privacy[2].

04 The distinction between privacy-related personal data and non privacy-related personal data is absent in the regulations on the protection of personal data. In this sense the latter complements the protection afforded by the right to privacy. To summarise one can say that all personal data are protected by the right to protection of personal data, whereas some of these data are also protected by the right to privacy. In practice, the ECtHR finds that most personal data use is covered by the right to privacy.

05 On a theoretical level, one can defend the view point that privacy law protects the opacity of the individual by prohibitive measures (non-interference), while data protection calls for transparency by the processor of personal data enabling its control by the concerned individuals, Member States and respective supervisory authorities (see below sub 7.). While privacy builds a shield around individual, creating a zone of autonomy and liberty, data protection puts obligations on the processor, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor's accountability.

1.1.2. Legal bases

06 At the international level, the right to privacy is protected by Article 12 of the Universal Declaration of Human Rights (1948)[3], however non-binding, and Article 17 of the International Covenant on Civil and Political Rights (1966)[4]. In 1980, the OECD issued the Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (4).

07 Protection of privacy and personal data at the European (regional) level is based on two systems. The first one (i.e. the Council of Europe (CoE)) is based on the Article 8 of the European Convention on Human Rights (ECHR) and sector-specific instruments, namely the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) (5) with an additional protocol regarding supervisory authorities and trans-border data flows (No. 181) (2)[5]. Besides, the CoE's Committee of Ministers adopted a

[1] European Convention on Human Rights (cf. Art. 8)
http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG
[2] e.g. Silver & Others v. United Kingdom (Applications Nos 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 and 7136/75) European Commission of Human Rights (1981) 3 EHRR 475 11 October 1980, S. and Marper v. The United Kingdom - 30562/04 [2008] ECHR 1581 (4 December 2008)
[3] Universal Declaration of Human Rights (cf. Art. 12 & Art. 29(2))
http://www.un.org/en/documents/udhr/index.shtml
[4] International Covenant on Civil and Political Rights (cf. Art. 17)
http://www2.ohchr.org/english/law/ccpr.htm
[5] Not all EU Member States have ratified yet, i.e. Belgium, Denmark, Finland, Greece, Italy, Malta, Slovenia nor the UK.

number of recommendations to its Member States concerning data protection (6). The ECHR establishes the European Court of Human Rights (ECtHR) in Strasbourg. While the ECHR itself does not mention protection of personal data, the ECtHR has developed this right from the right to privacy.

08 Not all fundamental rights can be considered absolute. Important for our purposes are the requirements imposed both by ECHR and ECtHR to assess legitimate interference with the right to privacy ('privacy test'). Following the wording of Article 8(2) ECHR[6], any interference must be:

a) prescribed by law (i.e. legality);

b) necessary in democratic society (i.e. necessity);

c) serve the certain public interest (i.e. legitimacy).

09 In other words, any interference must have a firm, clear, explicit and foreseeable legal basis[7] and must be proportionate to the legitimate aim pursued, i.e. must '*correspond to a pressing social need*'[8]. Some methods to assess lack of proportionality include manifest disproportionality or existence of an alternative and less intrusive solution. Proportionality requires that the interference does not go beyond what is necessary to obtain the objective and that no other less intrusive means exist to obtain that objective.

10 On the European Union level privacy is based on its Treaties, the Charter of the Fundamental Rights (CFR (1))[9] and secondary legislation, namely the Directives. After the entry into force of the Lisbon Treaty (6), the CFR became a legally binding instrument and the Treaties now include explicit reference to protection of personal data. The scope of application of the CFR is stated in Article 51(1) of this Charter: "The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law (…)"

11 Article 16 (*ex* Article 286) of the Treaty on the Functioning of the European Union (TFEU (7))[10] and Article 39 of the Treaty on the European Union (TEU (8))[11] both recognise the right to data protection. Article 7 of CFR provides the right to respect for private and family life and its Article 8 provides for the protection of personal data. The Court of Justice of the European Union in Luxembourg (colloquially the European Court of Justice, ECJ) ensures uniform application of the EU law.

12 The EU secondary legislation consist of three 'basic' instruments: the Data Protection Directive (95/46/EC (9)), the ePrivacy Directive (2002/58/EC (10)), as amended by Directives: 2006/24/EC (11) and 2009/136/EC (12), and the Data Retention Directive (2006/24/EC (11)). The 'specific' instruments consist of the Council Framework Decision 2008/977/JHA (13) (dealing with data protection with regard to criminal matters, i.e. former 3rd pillar) and the Regulation 45/2001 (14) (lying down data protection rules for the EU institutions and bodies). Note that the European Commission recently launched the process of the revision of the data protection framework[12] and that the ePrivacy Directive (15) is being reviewed and should be implemented by Member States 25 May 2011.

---

[6] (1) ,cf. Article 52(1) CFR.
[7] In other words, individuals should be able to predict with reasonable certainty when and under which condition such interference may occur. Hence the need for legal bases to be accessible and foreseeable are key features of the first requirement of the 'privacy test'.
[8] Cf. e.g. (17).
[9] Cf. Arts. 7-8 and Arts. 51-52, OJ C 83 of 30.3.2010, pp. 389-403 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF
[10] Cf. Art. 16, OJ C 83 of 30.3.2010, pp. 47-199 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF
[11] Cf. Art. 39, OJ C 83 of 30.3.2010, pp. 13-45 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:EN:PDF
[12] Cf. Note also that the Council of Europe considers the revision of the Convention No. 108 upon its 30th anniversary of signature (cf. (26)). So is said by the OECD with their 1980 Privacy Guidelines (17).

13 At the national level, provisions concerning privacy and data protection can be found in virtually all constitutions. With certain exceptions[13], all the EU Member States implemented all these Directives into their national legislation[14]. The ECtHR and ECJ jurisprudence regarding privacy and data protection is extensive[15] .

1.1.3. The EU Data Protection Framework

14 Following the structure of the Data Protection Directive, the Directive has been constructed as having a three-level system. The first level is the general one that applies to any processing of personal data (Sections I and II, articles 6 and 7 of Chapter II of the Directive). The second level, which needs to be applied on top of the first level, is applicable when sensitive data are being processed (Section III of Chapter II). The third level is applicable when personal data are being processed to third countries, i.e. outside the EU/EEA (Chapter IV of the Directive). The different levels of data protection within the EU are described in the following sections.

15 The Data Protection Directive (9) does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law (i.e. former 2nd and 3rd pillar of the EU) and by a natural person in the course of a purely personal or household activity (cf. Article 3(2) of the Directive).

16 Personal data shall mean '*any information relating to an identified or identifiable natural person*' (i.e. the 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*' (Article 2 of the Directive).

17 Two other categories of entities are defined by the Directive. The data controller is a '*natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*'. The data processor is '*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*'[16].

1.1.3.1. General Data Protection principles

18 General data protection principles from Directive 95/46/EC (9) also apply to Smart Grid data processing. The following principles are inferred from this Directive:

- **Fair and lawful processing** – Article 6(1)(a);
- **Data minimisation** – Article 6(1)(b) and (c):

    a) Purpose limitation:

        i) collected for specific, explicitly defined and legitimate purposes and not further processed in a way incompatible with those purposes – Article 6(1)(b);

    b) Data quality:

        i) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed – Article 6(1)(c);

        ii) accurate and, where necessary, kept up to date – Article 6(1) (d).

    c) Data needs to be retained only for as long as is necessary to fulfil that purpose ex Article 6(1)(c) (implicitly).

[13] For example, as of March 2011 the Data Retention Directive has not been yet implemented in Austria and Sweden. It was also rejected by the Constitutional Courts in Germany, Romania and the Czech Republic. Due to ECJ judgment on this matter changes may presently occur.
[14] Cf. (27) or (28).
[15] Concerning the former Court, cf. (29).
[16] The distinction between data controller and data processor might be sometimes problematic, cf. (30).

- **Legitimate basis** – Article 7: Personal data may be processed only if:

  a) the data subject has unambiguously given his or her consent[17] ; or

  b) performance of a contract: processing is necessary for the performance of a contract to which the data subject is party in order to take steps at the request of the data subject prior to entering a contract; or

  c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

  d) processing is necessary in order to protect the vital interest of the data subject; or

  e) processing is necessary for a public task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

  f) processing is necessary for the purpose of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interest are overridden by the interest of fundamental rights and freedoms of the data subject which requires protection under article 1(1);

- **Limitation of storage of data** – data are to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed – Article 6(1) (e).

- **Data security:**

  a) confidentiality of processing – Article 16;

  b) security of processing – i.e. appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing – Article 17;

  c) notification of processing data – i.e. controller must notify the supervisory authority before carrying out any wholly or partly automatic processing operation – Article 18(1);

  d) data breach notification – in addition to directive 95/46/EC directive 2002/58/EC (10) may be applicable: in case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, the data controller shall notify it to competent national authority – Article 4(3) of 2002/58/EC (amendment 2009/136/EC (12), entry into force: May 11, 2011).

1.1.3.2. Processing special categories of data

19 Processing of certain categories of data is prohibited, i.e. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life (Article 8(1) of the Data Protection Directive). Article 8(2) lists exceptions from this provision, i.e.:

- explicit consent of the data subject;
- obligations in the field of employment law;
- protection of the vital interest of the data subject where the data subject is physically or legally incapable of giving his consent;
- legitimate activities of a foundation, association or any other non-profit body;

[17] 95/46/EC Art 2 (h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

- when personal data were manifestly made public by data subject;
- purposes of preventive medicine, medical diagnosis, care or other treatment – Article 8(3).

20 Member States may, for reasons of substantial public interest, lay down exemptions in addition to the above mentioned (Article 8(4)). Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority (Article 8(5)). The Commission must be notified about such derogations (Article 8(7)). Processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression is allowed (Article 9).

21 The use of sensitive data in Smart Grids is currently not envisioned, but the rules and regulations on this subject apply to any development in this direction.

1.1.3.3. Transfer to third countries (i.e. outside EU/EEA)

22 Transfer of personal data to jurisdictions without adequate level of protection is prohibited (Article 25 of the Data Protection Directive), unless it is covered by one of the following exceptions – Article 26 (1):

- explicit unambiguous consent of the data subject;
- contract or pre-contractual measures;
- contract between controller and a third party in the interest of the data subject;
- legal requirement or necessity on important public interest grounds;
- necessity in order to protect the vital interest of the data subject;
- transfer from a public register;
- authorisation by Member State – Article 26(2).

23 The European Commission determines what jurisdictions provide the adequate level of protection (Article 25 (6))[18].

1.1.3.4. Sector specific rules and regulations

24 There are a number of rules and regulations that may be of special relevance to the energy sector by alignment with other sectors (such as telecommunications or market regulation):

a) **ePrivacy Directive –** regulates the processing of personal data and the protection of privacy in the electronic communications sector, namely the traffic and location data:

i) **traffic data** – any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof – Article 2(b). The principal rule is to erase or anonymise as soon as possible – Article 6(1), with the following exceptions:

(1) billing and interconnection payments (Article 6(2)),

(2) consent of subscriber (user), provided it is necessary for marketing of provider's own electronic communications services or provision of value added services; yet subscriber (user) can withdrawn their consent at any time (Article 6(3)),

(3) in any case: obligation to inform subscriber (user) prior to obtaining consent (Article 6(4));

[18] The current list can be found at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

ii) **location data** – any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service – Article 2(c):

(1) note that this concept might overlap with traffic data (thus Article 6 might apply also),

(2) principal rule: processing only allowed if made anonymous and with consent of user or subscriber for the provision of a value added service (Article 9(1)),

(3) withdrawal of consent at any time (Article 9(1)), as well as temporary refusal of processing (e.g. during holiday) (Article 9(2)),

(4) data subject (user) must be informed about: type of location data, purposes of processing, duration of processing and transmission to third party, if applicable (Article 9(1));

iii) **data breach notification** – in case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the data controller shall notify it to competent national authority – Article 4(3) (entry into force: May 11, 2011). Moreover, when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay;

b) Data Retention Directive – regulates the data retention period regarding publicly available communications services and public communications networks:

- aim is to ensure data are available for investigation, detection and prosecution of serious crime (yet the definition of 'serious crime' is left for the Member States);
- applicable to traffic data and location data on legal identities and natural persons;
- not applicable to content of electronic communications (Article 5(2));
- requires retention of certain data for the period between 6 and 24 months,
- these data include data necessary to:
  - trace and identify the source and destination of a communication;
  - identify the date, time, duration and type of a communication (i.e. which telephone or internet service);
  - identify users' communication equipment or what purports to be their equipment;
  - identify the location of mobile communication equipment.
- data shall only be provided to competent national authorities (Article 4), yet this does not provide guidance for national law on the conditions under which law enforcement agencies can access retained data; note also that a number of national implementations of this Directive has been struck down by the respective supreme or constitutional courts (Germany19, Romania and recently Cyprus);

c) Self-regulation

- e.g. the European Code of Practice for the Use of Personal Data in Direct Marketing (16).

[19]Cf. (42).

1.1.4.Rights of the data subject

25 Data subjects have the following rights regarding processing their personal data, as[20]

- the right to be informed about processing their personal data in a clear and understandable language – Article 12(a),
- the right to access to own personal data – Article 12(a),
- the right to rectify any wrong or incomplete information – Article 12(b),
- the right, in some cases, to object the processing on legitimate grounds – Article 14,
- the right not to be subject to an automated decision intended to evaluate certain personal aspects relating to the data subjects as their performance at work, creditworthiness, reliability, conduct – Article 15,
- the right to judicial remedy and to receive compensation from the data controller for any damage suffered (short of vis maior) – Article 22 and Article 23, respectively.

26 These data subject's rights correspond to the data controller's obligations to:

- ensure the data subject's rights are duly observed;
- ensure observance of the data minimisation principle;
- ensure observance of the criteria for making the data-processing legitimate (e.g. consent or performance of the contract);
- safeguard confidentially of processing;
- safeguard security of processing;
- notify processing of personal data to the national data protection authority (DPA);
- in case of the transfer to the third countries – ensure if these countries provide adequate level of protection (in general)), or in case of derogation ensure that the conditions of Article 26 of Directive 95/46/EC are met;

1.1.5.Relation between the concepts of privacy and data protection

27 It follows from the EU Charter of Fundamental Rights (CFR (1)) that there is a formal difference between privacy and data protection. On the one hand, Article 7 CFR establishes everyone's right to privacy as a right '*to respect for his or her private and family life, home and communications'* in almost the same terms[21] as Article 8(1) of ECHR. Article 8 CFR constitutionally hallows the right to the protection of personal data. In other words, the Charter distinguishes two rights of which the former concerns the privacy of individuals while the latter focuses on the processing of personal data and provides that such processing should be surrounded with (constitutional) safeguards.

28 Since Article 7 CFR is virtually a replica of Article 8 ECHR at European level the content of privacy for legal purposes can be securely derived from the pertinent case law of ECtHR, which has ruled that Article 8 ECHR – with its four components private life, family life, home and correspondence – can cover a wide range of issues such as integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, gender, health, identity (i.e. a right to have some control over identity markers such as one's name), sexual orientation, protection against environmental

[20]Cf. (9).
[21] The CFR mentions the more up-to-date term of *'communications'* instead of *'correspondence'* in the ECHR.

nuisances and so on: the list is not exhaustive. The ECtHR affirmed that it is neither possible nor necessary to determine the content of privacy in an exhaustive way[22]. It also implied that privacy is a relational concept that goes well beyond a mere right to intimacy, with the important consequence that Article 8 rights may also protect visible and public features and conduct of individuals (public privacy)[23]. Progressively, the Strasbourg Court also acknowledged the right to make essential personal choices (such as name and sexual orientation)[24] and eventually this has led the Court to state that individual self-determination or autonomy is an important principle underlying its interpretation of Article 8 ECHR[25]. In this sense, the Court seems to favour a 'liberty' rather than a 'bundle of subjective rights' approach to privacy.

29 Privacy and data protection are thus different, but they are certainly not unrelated. They are intertwined and overlapping, but their respective scopes and regimes should be distinguished.

30 As a matter of fact, the ECtHR did effectively look at data protection cases through the prism of privacy (Article 8 ECHR) and it has developed criteria to assess whether an issue of data protection touches or not upon the right to privacy. The Court thus distinguishes between the processing of data that are constitutive of the private life and the processing of data that are not. It uses two criteria to make the distinction: the nature of the data processed and the extent of the processing. If the data are intrinsically linked to the private life of the individual, then the processing will fall under Article 8 ECHR without further doubt. If the data are not 'essentially private', one will have to look at the extent of the processing: does it systematically store the data, does it store the data though not systematically, with a focus on the data subject, or could the data subject not reasonably expect the processing? In a number of cases, the Court has condoned data processing to issues pertaining to the privacy of the data subject[26]. Contrary to data protection, which directly applies every time 'personal data' are processed, privacy protection ex Article 8 ECHR does not. And that means that not every processing of personal data, which resorts under data protection legislation, necessarily affects privacy. But it will be protected through data protection nevertheless.

31 Where the Strasbourg Court has acknowledged that a data protection is also a privacy issue, it has granted some of the guarantees foreseen in data protection legislation: it has acknowledged a right to access to personal files[27], claims regarding the deletion of personal data contained in public dossiers[28] and the correction of

---

[22] ECtHR, Niemietz vs. Germany, 13710/88, paragraph 29: *'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.'*

[23] E.g., Rotaru 2000, P.G. & J.H. v the UK 2001, Peck.

[24] ECtHR judgment of 16 November 2004, Unal Tekeli v. Turkey, appl. no. 29865/96, S. and Marper v. the United Kingdom, appl. nos. 30562/04 and 30566/04 and ECtHR [GC] judgment of 22 October 1981, Dudgeon v. the United Kingdom, appl. no. 7525/76.

[25] Pretty, paragraph 61 *'As the Court has had previous occasion to remark, the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person [X. and Y. v. the Netherlands, paragraph 22]. It can sometimes embrace aspects of an individual's physical and social identity [Mikulic v. Croatia, 53176/99, paragraph 53]. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 [B. v. France, paragraph 63; the Burghartz v. Switzerland, paragraph 24; Dudgeon v. UK, paragraph 41, Laskey, Jaggard and Brown v. UK, paragraph 36]. Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world [Burghartz v. Switzerland, paragraph 47; Friedl v. Austria, paragraph 45]. Though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.'*

[26] De Hert P. & Gutwirth S. (2009) 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action,' Gutwirth S. et al. (eds.), Reinventing Data Protection?, pp. 3-44; De Schutter, Olivier, 'Vie Privée Et Protection De L'individu Vis-À-Vis Des Traitements De Données À Caractère Personnel', R.T.D.H.: 148 et seq.

[27] ECtHR, Gaskin v UK, 10454/83; ECtHR, Antony & Margaret McMichael v UK, 16424/90; ECtHR, Guerra et al. v Italy, 14967/89; ECtHR, McGinley & Egan v UK, 21825/93 and 23414/94.

[28] ECtHR, Leander . Sweden, 9248/81; ECtHR, Segerstedt-Wiberg et al. v Sweden, 62332/00.

'official sexual data' from transsexuals[29]; it has further insisted upon the necessity of having independent supervisory authorities in the context of the processing of personal data[30]; it endorsed the principle of purpose limitation when it ruled that personal data cannot be used beyond normally foreseeable use[31], and that governmental authorities may only collect relevant data based on concrete suspicions[32]. Finally, the Court acknowledged the right to financial redress in the case of a breach of Article 8 ECHR caused by the processing of personal data[33].

32 The ECJ is competent to make rulings concerning conflicts based upon the Data Protection Directive. Some of its cases have been permeated by a 'privacy logic'. In Österreichiser Rundfunk (2003)[34], the Court has stated that the processing of personal data can affect the right to privacy. Therefore, provisions of the Directive that might affect this right must be interpreted in the light of Article 8 ECHR (paragraph 68) and must pass the threefold threshold test foreseen by this article, although Member States enjoy a wide margin of appreciation latitude (paragraph 83). In its first judgment, the Court went even so far as to declare that an unlawful data processing is equal to a breach of privacy (paragraph 91). References to the threefold test of the ECHR were also made in other cases[35]. However, in more recent cases, the Court of First Instance[36] reminded us that *'the mere presence of the name of a person in a list of participants at a meeting does not compromise the protection of the privacy of the person'*[37].

33 Finally, in their conceptual relationship, it is important to underline that data protection is both broader and narrower than privacy. It is narrower because it only deals with personal data, whereas the scope of privacy is wider. It is broader, however, because the processing of personal data can have consequences not only in terms of privacy, but also in terms of other constitutional rights. For example, data processing can impact upon people's freedom of expression, religion and conscience, voting rights, etc. Most importantly, the knowledge about individuals that can be inferred from their personal data may also bear the risk of discrimination.Roles and responsibilities

34 In the legislative process in the EU involved are: the Commission, the Parliament, the Council, the Economic and Social Committee and the Committee of Regions. In the European Commission, the Directorate-General for Justice (DG JUST) is competent for fundamental rights, therefore comprising data protection (Data Protection Unit C3). In the European Parliament, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) deals with the privacy and data protection issues. For the deployment of smart metering (and Smart Grids in general) in the EU responsible is the Directorate-General for Energy (DG ENER), in particular the Direction for Security of Supply and Energy Markets.

35 The Data Protection Directive (9) establishes:

- national data protection authorities /commissioners (DPA) – i.e. one or more public authorities responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Directive (Article 28);

- Working Party on the Protection of Individuals with regard to the Processing of Personal Data (the so-called Article 29 Working Party). The working party is an advisory body with the obligation to advise the Commission on any eventual amendment of the Data Protection Directive, as well as with the right

[29] ECtHR, Rees v UK, 9532/81; ECtHR, Cossey v UK, 10843/84; ECtHR, B v France, 13343/87; ECtHR, Goodwin v UK, 28957/95.
[30] ECtHR, Klass v Germany, paragraph 55; ECtHR, Leander v Sweden, paragraph 65–67; ECtHR, Rotaru v Romania, paragraph 59–60. See in detail: E. Brouwer, o.c., 143–144; ECtHR, Gaskin v. UK, 10454/83; ECtHR, Z. v Finland, 22009/93.
[31] ECtHR, Peck v UK, paragraph 62; ECtHR, Perry v UK, paragraph 40; ECtHR, P.G. & J.H. v UK, paragraph 59. More in detail: E. Brouwer, o.c., 138–139.
[32] ECtHR, Amann v Switzerland, paragraph 61 and paragraph 75 ff.; ECtHR, Segerstedt-Wiberg v. Sweden, paragraph 79.
[33] ECtHR, Rotaru v. Romania, paragraph 83.
[34] Cases C-465/00, 138 and 139/01 *Rechnungshof v. Österreichischer Rundfunk* ECR I-12489.
[35] ECJ, Opinion of the Advocate General, Cases C-317/04 and C-318/04, paragraph 229.
[36] Now the General Court.
[37] ECJ, The Bavarian Lager Co. Ltd v Commission of the European Communities, paragraph 114-115.

to make recommendations on its own initiative on *'on all matters relating to the protection of persons with regard to the processing of personal data in the Community'* – Article 30(3). The Working Party has already issued a considerable number of opinions and recommendations concerning protection of privacy.

36 Article 41 of the Regulation 45/2001 (14) establishes the European Data Protection Supervisor (EDPS), who supervises the EU institutions, bodies, offices and agencies. (However, he has no oversight over the national data protection authorities.) He also provides consultation and ensures cooperation in the field of data protection in the EU.

37 Certain Member States have established the institution of data protection officer for certain private bodies (e.g. Germany and the Netherlands)[38]. His duty is to ensure observance of the data protection laws within a business. Note also impact of think-tanks, other non-governmental organisations (NGO) and academia in the debate on privacy and data protection.

1.1.6.EU and National Legislation Authorities

38 Legislation authorities are in charge of defining legislation and metrics for areas such as environmental policy, social policy, energy policy and economic policy. They are also responsible for the authorisation needed to develop the power grid infrastructure.

39 Policy makers should ensure active support for market and competitive business activities – including innovative approaches where these benefit their citizens. They must put in place the appropriate regulatory framework and develop and implement a strategy to protect customers and enable them to access the full benefits of Smart Grids and smart metering. Member States should be required to report on the costs and benefits to consumers of the smart meter rollout.

40 Including the discussions and work of Expert Group 3 (17), the following areas have been identified as priority areas to be addressed:

- Given that the marketplace will expand with new actors and services offered, the required legislative framework needs to exist and be enforced to ensure all relevant market rules and regulations are in place between TSOs, DSOs and other market participants.
- Policy makers and regulators will be required to create a framework and guidance for the smart metering roll-out, to deal with issues including customer data privacy, data protection, tariffs, remote management and disconnection. Necessary legislation for ensuring industry standardisation and MID compliance within Member States will be required.
- The TEN-T Guidelines[39] have set clear priorities for the development of transmission grid infrastructure for the EU. Policy makers will be required to ensure the required legal framework exists to support this.
- As distributed generation will further grow, DSOs will have to rely on it to contribute to the stability of the overall grid and the associated regulatory framework to both incentivise and enforce these changes will need to be created.
- Defined and enforceable legal provisions for education and certification of DSOs and TSOs staff as well as training of other market participants will need to be developed (e.g. comparable to provisions in air-

[38] Cf. sections 4f and 4f of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSmart Grid), at http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSmart Grid__idFv01092009.pdf?__blob=publicationFile and the Dutch Association of Data Protection Officers (Nederlandse beroepsvereniging van Functionarissen Gegevensbescherming, NGFG), at http://www.ngfg.nl/.
[39] The TEN-T Guidelines are the general reference framework for the implementation of the transport network and for identifying projects of common interest. The guidelines aim at integrating national networks and modes of transport, linking peripheral regions of the European Union to the centre, and improving safety and efficiency of the networks. Decision no 1692/96/ec of the European Parliament and of the Council of 23 July 1996 on Community guidelines for the development of the trans-European transport network.

traffic control today). The goal will be to ensure an efficient and secure operation of highly meshed energy grids of Europe.

1.1.7. Regulators

41 Regulators are independent bodies responsible for the definition of framework (market rules), for setting up of system charges (tariffs), monitoring of the functioning and performance of energy markets and undertaking any necessary measures to ensure effective and efficient market, non-discriminative treatment of all actors and transparency and involvement of all affected stakeholders.

42 It is important that national regulatory authorities and European institutions (CEER, ERGEG and ACER in the future) ensure a long-term-predictable and stable regulatory framework, including adequate incentives for investments.

43 The emergence of electric vehicles is expected to become an important factor in the electricity supply chain, with the emergence of multiple new business models for 'mobile' customers. This may in turn result in the need for increased regulatory oversight, similar to the recent developments in the telecommunications industry.

44 Regulators should also be assigned the responsibility for systematically reviewing customer protection to ensure that it is fit for purpose in a smart world. For example, specific new safeguards may need to be put in place to protect customers from misuse of remote disconnection, remote switching, misselling of complex new tariffs, alongside the revised Data Protection Directive and privacy and security rules. Regulators have a particular responsibility to protect the interests of low income and vulnerable customers to ensure that all customers are able to access the benefits of Smart Grids and smart meters on an equal basis.

45 Regulators must undertake regular monitoring of the progress of smart meter rollout, with particular reference to the consumer experience, complaint handling and redress, and reporting on the costs and benefits to consumers of rollout. Reporting should also include progress on delivery of the Member State's impact assessment for smart metering and include estimated energy and carbon dioxide reduction.

46 The development of energy services markets is likely to result in the increasing bundling of services offered to customers. Consideration should be given to the regulatory framework to ensure that customer complaint handling and redress is simple and effective. Member States should review their regulatory frameworks to ensure they reflect the needs of the smart energy world.

47 In general, the investment costs in the electricity grids are covered by grid tariffs. These include among others the use of system charges, access charges, connection charges, metering charges, etc. The costs in the grid need to be as far as possible attributed to those incurring them. The transparent cost structures on both transmission and distribution level need to foster the development of Smart Grids. The first mover[40] needs not to be burdened with the total cost of a change which further users will then access for free. Regulation of outputs, by incentives, by minimum requirements or by a combination of both, requires predefined performance targets and indicators.

48 In the European context a number of different public funding options are in place ranging from EU funding, national governments funding, both as the sole option or in combination with public-private partnerships. Public subsidy should only be used where it is clear that industry will not invest otherwise and – most important – where the benefit to society clearly justifies such an approach. The type of funding to be used will also depend on the stage when it is needed, e.g. initial R&D phase, pilot demonstration projects, transition phase from first market introduction to a fully-fledged deployment.

49 Defining metrics for quantification of the effects and benefits of Smart Grids – with specific emphasis on the evaluation of efficiency, effectiveness and comparative cost analysis in relation to a conventional 'non-smart' approach – is a challenging but necessary task in order to be able to perform the cost / benefit analysis, before cost recovery and possible introduction of incentives for the deployment of Smart Grids. This is a complex and

[40] First movers need not create barriers for entrance.

high priority issue which needs to be addressed accordingly by the regulators in close cooperation and coordination with power grid users, owners and operators.

50 The European Energy Regulators, CEER, have worked on issues of smart metering and smart grids for some time. Furthermore the duties for member states and energy regulators as regards to ensuring interoperability and the deployment of smart meters and smart grids is strengthened through the 3rd package.

CEER has in 2011 made recommendations on regulatory aspects of smart metering for electricity and gas, E10-RMF-29-05. In these recommendations CEER defines what smart metering would deliver to customers in the form of energy services and what to consider when conducting a roll-out and CBA. There are a number of functionalities that needs to be in place in order for these services to be enabled. The recommendations are a direct result of the 3rd package provisions regarding intelligent metering systems and consumption information to energy customers. Furthermore in 2010 CEER has defined the concept of smart grids, E10-EQS-38-05 , and also made a status review on the regulatory aspects of smart grids so far, E11-EQS-45-04.

1.1.8. Competition authorities

51 To safeguard general access to electricity networks, competition authorities have the task to monitor tariffs and conditions and enforce compliance to the regulatory framework as to ensure non-discriminatory tariffs and conditions. By monitoring and enforcing compliance, competition authorities make sure that the market is accessible not only to all consumers, but also to new market parties. Accessibility of the market is vital in order to allow increasing decentralised production, accessible prices and utilisation of Smart Grid opportunities.

52 Furthermore, competition authorities have an important signalling function to the regulators. Whenever the regulatory framework is not providing the required conditions for a well-functioning market, competition authorities inform regulators of necessary measures to be taken.

1.1.9.Legislation for products participating as actors in Smart Grid

53 There is harmonised regulation for products brought into the EU common market, defining the legal essential requirements for all harmonised products that are provided to the common market.

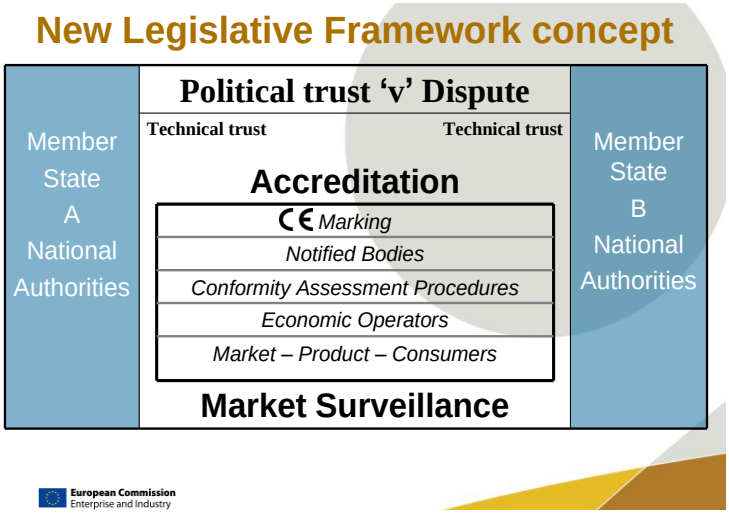

Figure 1: The New Approach / NLF Concept

(Source: Rita L'Abbate DG ENTR European Commission)

54 The detailed product requirements are mandated by the European Commission, and listed on the Official Journal of the European Union for standards that provide the presumption that compliance to the standard ensures that the products comply to the essential requirements as defined in the regulation (New Approach concept)) (18)) that is a commitment by the regulators on how new regulation for products is to be written (i.e. it provides specific modules to be used in legislative texts). The decision furthermore defines obligations and

responsibilities as well as options on conformity requirements for products for all economic operators that provide products to the market – manufacturers, importers, distributors and traders.

55 Those product specific regulations are either sector specific or the regulation is horizontal / hazard based – and applies to all harmonised products of all sectors; therefore all products need to comply to those horizontal regulatory requirements as well. The following figure illustrates this interdependence (i.e. for MID related products):

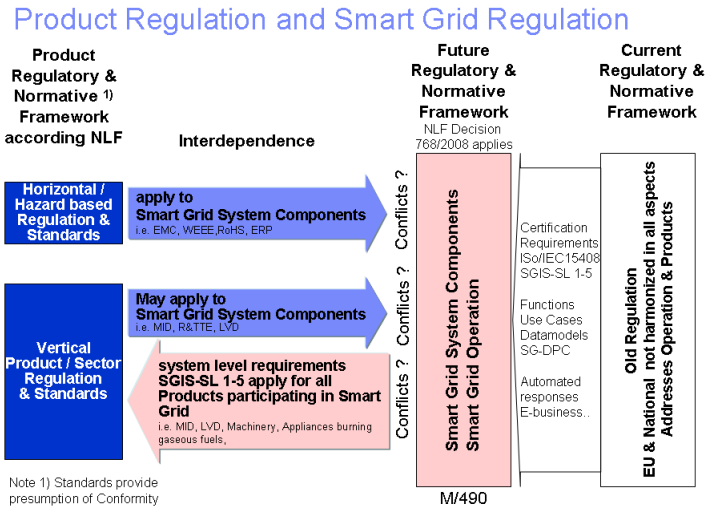

Figure 2: NLF Product Regulation versus Future Smart Grid Regulatory& Normative Framework

(Source: German Smart Grid research demonstration project: moma)

56 The NLF also specifies that the New Approach concept will be used for regulation – i.e. that mandates require European Standards Organisations (ESO) to provide product standards that describe product requirements in detail to assure that the product specifications cover the essential requirements in such a way that conformance to the standards provides the presumption of conformity to the essential requirements as outlined in the legal text. There is a process in place to safeguard this at EU and ESOs.

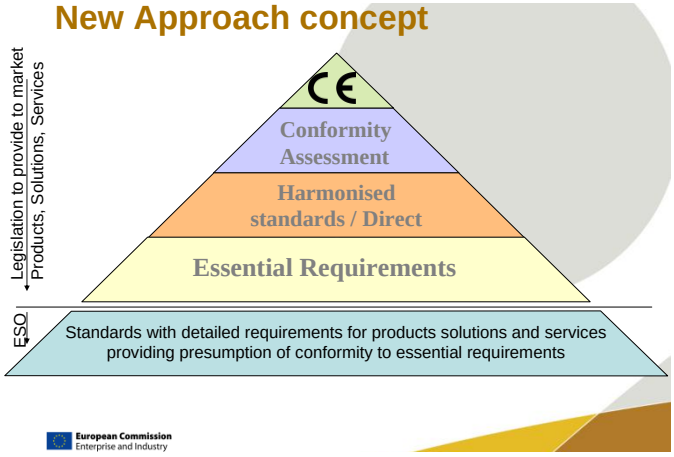

Figure 3: The New Approach / NLF Concept

(Source: Rita L'Abbate DG ENTR European Commission)

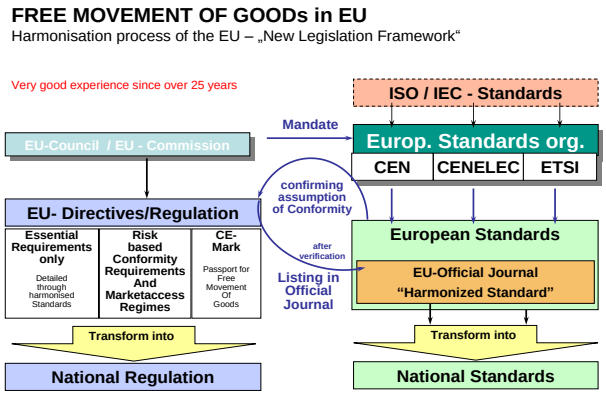

Figure 4: NLF - EU versus National regulation & Standards

(Source: Public Domain knowledge capture by A. Malina)

57 Besides the product regulation there is regulation that addresses the usage phase of products – i.e. the privacy /data protection requirements. These operation oriented legal texts do not provide specific requirements in respect to product design, manufacturing and bring to market – conformity requirements. The current regulatory requirements for the Energy Sector includes both – operational and product requirements.

58 Products that will eventually be integrated into the Smart Grid will interact with energy management services and interoperate as new actor / system component will need to fulfil appropriate Smart Grid security requirements as required by the use cases and data models.

EG2.G.1 The European Smart Grid regulation should utilise and implement decision 768/2008/EC as it will need to be harmonised to products already harmonised under NLF. This should be the case for all products that will be interchangeably integrated and that should seamlessly interoperate as actor in the Smart Grid with other system components of the Grid.

1.1.10. Standardisation Bodies

59 Standardisation bodies are responsible for standardisation of all relevant elements and components within the electricity supply chain. This leads to harmonisation and interchangeability of relevant energy services, supports removing barriers to trade, creates new market opportunities and reducing manufacturing costs.

60 An open and standards based approach is crucial for the deployment of Smart Grids. The recognised European Standards Organisations (ESOs) CEN, CENELEC and ETSI are traditionally closely linked to regulation at European level, providing the technical specifications that are needed to implement regulation. These links are explicit in the context of EU Directives including those for EMC (Electro-Magnetic Compatibility), low-voltage and (in relation to Smart Metering) measuring instruments (Directive 2004/22/EC on Measuring Instruments (MID) (19)).

61 The ESOs maintain formal links with global standardisation bodies ISO, IEC and ITU-T (and also with UN-ECE, which is relevant for electronic business process standards) and those links should be utilised to avoid duplication of activities and possibly conflicting standards at the European or a wider level. Whereas some issues can only be standardised at European level, in other cases the necessary standards should be provided globally. However, the ESOs should ensure these global standards meet European requirements.

62 In the ICT standardisation, there is a plethora of different industry consortia providing sometimes competing standards solutions, and care needs to be taken to avoid inter-operability problems or issues related to intellectual property rights.

63 Standardisation should play a role also in other areas where technical enforcement for market decisions by regulators or private sector actors is needed. Moreover, standardisation organisations have to provide the needed flexibility to accommodate with the increasing variety of business models. These needs must be based

on an agreed set of use-cases to be developed and maintained over time. All of those use-cases should be based on the described actors and roles.

EG2.G.2 Following a clarification of the relationship between the standards produced by the ESOs under the standardisation mandate and future legislative initiatives at the European level, the Standards need to be developed by standardisation organisations based on a common set of use-cases taking into account the different business models across the Member States. The standardisation organisations will maintain these standards over time as Smart Grid applications evolve.

1.1.11. Enforcement

64 Enforcement plays a vital role in achieving the Smart Grid benefits offered by relevant directives, laws, regulations and standards. Effective enforcement can protect the Smart Grid transition, it can deter violations of law and it can encourage improved performance by the regulated community. A good enforcement program also reinforces the credibility of protection efforts and the legal system that supports them and ensures fairness for those who willingly comply.

65 European guidelines can be a complementary tool to strengthen enforcement. They emphasize that opportunities for such strengthening exist at the local, national and EU level. Action at the national level is crucial and is given emphasis, but guidelines may also acknowledge an effective implementation of Commission decisions ordering Member States to comply with Smart Grid relevant directives, laws, regulations and standards. In particular there should be effective monitoring and enforcement mechanisms in place to ensure that smart meter rollout is delivering the anticipated benefits to consumers and citizens.

66 As noted, the development of the Smart Grid and with it growing energy services markets and smart homes is likely to result in the increasing bundling of services offered to customers. When things go wrong, the governance responsibilities are split across a number of regulators – those for telecom, energy, products and services. This can be confusing for customers and hard for them to navigate if they have a problem and want to seek resolution. Consideration should be given to the regulatory frameworks along a – preferably newly developed – integrated governance model for Smart Grids to ensure that customer complaint handling and redress is simple and effective. Member States should evaluate their regulatory frameworks on Smart Grids and consumers to ensure they reflect the needs of the smart world and the consumers.

EG2.G.3 Enforcement is a key aspect of regulation. There are many relevant authorities within the European Union at the different organisational levels. In order to be able to effectively enforce regulation guidelines need to be developed on monitoring and enforcement. It is recommended to address the Member States to review their regulatory frameworks in order to be able to enforce the use of common standards across the European Union.

2. Privacy in Smart Grids

67 The privacy issues associated with the introduction of Smart Grids deserve special attention. Certain (personal) data may be relevant to more than one party within a country or across countries. The deployment of Smart Grids and smart meters thus prompts decisions at (at least) a national level about the requirements of the various market participants, the nature of data (individual or aggregated) and how data flows should be managed and secured. In relation to the data from smart metering, some of the data will be necessary to suppliers for services around the supply of energy, e.g. the provision of accurate[41] consumption and energy production information and billing, debt management and theft prevention or detection. For any detailed information or other data needed in order to offer services clearly beyond original purposes, explicit consent from data subjects is required. This view is also shown in WP183 of the Article 29 Data Protection Working Party (20). Article 29 Working Party further recommended developing effective and practical means by which data subjects can express their consent.

68 DSOs and energy suppliers acting as enablers of demand side response may maintain information hubs. Customers should be able to access their historic energy consumption information for free in a format that allows them to make like for like comparisons with tariffs and deals available in the market. The responsibility for administration of verified and validated master data currently lies with the DSO in most European countries. The main exception to this are the UK and Germany where energy suppliers are likely to be responsible for administering most meter level data, with the exception of certain limited (e.g. registration) data held by a central data communication company. It should be ensured that consumers have control over their data to the extent data protection and other legislation specifies; this includes what data is read from the meter, who is collecting it and for what purpose. Personal data should under no circumstances be saved or shared with other market actors beyond national law or what is agreed between consumer, energy provider or 3rd parties contracted by the consumer.

69 Managing the protection of personal data is important: such protection is mandatory under the EU data protection Directive (95/46/EC (9)) and the national data protection legislations as well as under the fundamental right to the protection of personal data has been enshrined in Union law in the Charter of Fundamental Rights which enshrined the fundamental right to the protection of personal data in Union law (Article 8 CFR). Moreover, national data protection legislation and individuals (data subjects) demand that their data will be handled appropriately[42]. Inappropriate or unauthorised processing of personal data can damage the reputation of the supplier and trust relationships between the data controllers and the data subjects (for example, relationships between customers and their suppliers, employees and their employers and citizens and government institutions) and it may cause harm, both material and non-material to consumers..

70 Personal data is defined by directive 95/46/EC article 2(a): 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject') as described in chapter 1.1. , 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.

71 Market participants can process personal data if they establish the compelling legitimate purpose under article 7. The Member State 'supervisory authority' should be notified in accordance with Article 18. Member States shall determine more precisely the conditions under which the processing of personal data is lawful.

[41] For detailed information, consent is required.
[42] Distrusting data handling is a growing concern. Data controllers, other parties in the sector and government institutions need to show and prove compliance by making it transparent and visible.

EG2.P.1 The introduction of Smart Grids with intelligent meters changes the polling frequency of measurement and the coverage of the measurement at the consumer location. Whereas up to now the frequency is low and covers an area or larger number of energy users, the intelligent meter may revolutionise the frequency to minutes or real-time whereas the coverage is in the order of individual consumers or households. This implies that where up to now the operator has a broad view of the energy behaviour of a larger set of consumers, this view will evolve to detailed information on the energy behaviour of sole end consumers. Because of this shift in detail it is recommended to confirm that in accordance with opinion 183 of the Article 29 Data Protection Working Party most data from Smart Meters can be considered personal data and to determine the extent to which the various data at different levels of detail can be considered as such.

EG2.P.2 The implementation of Smart Grids potentially connects location information to specific data that holds information on the use of electrical energy, and in the future possibly more. The fingerprint or contents of this data provides information on what is going on at the location at a specific moment, and may show patterns over longer time which may have great impact on the privacy and security of the consumer. It is recommended that adequate measures are deployed to protect the contents and nature of this data in order to safeguard the privacy of the consumer.

2.1. Privacy and Data Protection challenge

72 Seeing the move from the electricity grid towards the 'Smart Grid' as a single project, this project is unprecedented in terms of scale and complexity. This weighs even heavier as we are dealing with critical infrastructure, in some cases unclear goals, some players moving into domains they have little experience in, a potentially huge privacy impact and an in-vivo implementation.

73 While the scope of this analysis is security and privacy related gaps, those are in this case inseparable from architecture and management issues – if parts of the overall project struggle, security and privacy guards should not be pushed back. While these matters are often not initially included, privacy and security flaws are often pointed out to the politicians as important issues.

74 The privacy and data protection challenges should be approached in a systemic way, filling the gaps between the available solutions leadingto a fully functional whole based upon a security and privacy vision and related architectural blueprint.

2.1.1. Privacy Enhancing Technologies

75 Privacy protection has a long history, starting before modern computer technology. Traditional mechanisms for privacy protection focus strongly on regulation, imposing conditions on storage and restricting use of personal information[43]. In an internal market data should flow freely, but also fundamental rights, such as the one to data protection, should be guaranteed: at best this information could be anonymised or at least access to it should be regulated and protected.

76 Modern data mining technologies significantly undermine the effectiveness of these protection mechanisms. It has been shown that allegedly anonymous datasets can easily be de-anonymised (21). For example, L. Sweeney shows that 87% of the US population are uniquely identified by the combination of gender, birthdate and postal code, which she used to de-anonymise published medical records (22). Another example was the publication of AOL search data for research purposes, which immediately lead to the identification of a number of users by bloggers (11). Similarly the publication of an anonymised dataset by the Netflix service was followed by award winning techniques by Shmatikov et al showing how it can be de-anonymised (23).

77 In the Smart Grid setting, the de-anonymisation and inference risks have not yet been investigated. What is known for sure is that a number of categories of demographics can be derived with good certainty (e.g. number of people in a household, age and income brackets of the inhabitants, number of working household members,

[43] The Article 29 Working Party has stated in (34), p.13: *'The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), privacy by default settings and the necessary tools to enable users to better protect their personal data (e.g. access controls, encryption)'.*

some information about the occupation). These suggest the threat of de-anonymisation is serious. It is also clear that complete identification of most datasets is possible if rich side information such as credit card data is available.

78 While modern data mining technologies undermine classic protection, new advances in cryptographic techniques have become practical, and allow us to build systems that do not require the sharing of personal information. In a nutshell, it has become possible to compute almost arbitrary functions on encrypted data, i.e. the entity that handles the data never learns any input, only the result of the computation (the earliest example of this was called the millionaires problem where two millionaires want to determine who is richer, without revealing their actual wealth). By now, such protocols have entered practical use, for example in establishing the market clearing prices for Danish farm goods (2), and in the Trusted Computing Standard (24) (the latter case is especially interesting, as this was a case where the original solution was heavily criticised by privacy organisations and the Article 29 Working Party (see also footnote), and the use of anonymity preserving cryptography made the technology acceptable). For the Smart Grid scenario, protocols have been proposed that allow for secure computation of the monthly energy bill without revealing individual readings (6), and to aggregate measurements from several meters for load management purposes (7).

2.1.2. Business Continuity Plans

79 It is necessary that on all levels, a continuity plan is developed to assure the functionality of the Smart Grid once incidents occur, as this may have a large impact on the grid and its users. This plan needs to be included into the architecture - for example, it may be necessary to have the ability to turn of the 'smart' part of the grid and keep a non-smart component working and an ability to verify properly or improperly functioning devices remotely.

2.1.3. Privacy by Design and by Default

80 Privacy by Design is considered to be the use of suitable standards and principles to ensure the fundamental right of individuals in order to enable them to control the use of their personal data (see also e.g. 1.1.4). It also ensures that the appropriate safeguards are put in place by the controller or processor in order to protect the personal data. The Privacy by Design principle should be integrated in the project governance framework and can proactively embed all privacy requirements into their designs in order to prevent the occurring of events that invade the privacy of subjects. Privacy can be made a core functionality in the design and architecture of Smart Grid systems and practices, where appropriate measures and a high level of protection of personal data are considered the default.

81 It has been shown in recent research that the classical privacy controls – e.g. anonymisation and access control solutions – have structural limits in providing consumer privacy. Modern technologies have been developed lately, some of them especially with Smart Grid applications in mind. These developments need to be integrated into the overall architecture, and more research is needed to assure all Smart Grid use cases are covered.

82 Privacy by Design must ideally become an organisation's standard mode of operation, by deploying a triad of encompassing privacy enhancing technologies, systems and practices:

a) IT systems;

b) accountable business practices;

c) physical design and networked infrastructure.

83 The Article 29 Working Party has stated in its opinion WP 168 on The Future of Privacy p.13: 'The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), privacy by default settings and the necessary tools to enable users to better protect their personal data (e.g. access controls, encryption)'.

84 As history shows us, a functional creep is likely to develop overtime, pushed forward by new technologies. The early functions of the Smart Grid will finally be replaced by even smarter functions. Embedding Privacy by Design and by Default principles in this initial stage will make it possible to enhance the Smart Grid in the

future, without the loss of security. Privacy by Design needs to cover the whole information system of the Grid, from meter to back-office, to support, to the financial department. This requires enforcement of information coordination and involvement of the right expertise throughout all areas of the Smart Grid system. The roadmap must pay specific attention to the Privacy by Design principles.

85 According to responses to questions to several DPAs privacy by design is generally promoted. Including assessment of privacy risk and measures to mitigate this risk early on in projects can significantly reduce the cost associated with implementing additional measures to adequately protect privacy later on.

86 The promotion of this principle can be an important part of the communication with parties within the sector. This includes suppliers and contractors that may be responsible for parts of the design of the infrastructures. By promoting a dialogue and a sector wide approach in the design of infrastructures privacy risks can be reduced while minimizing the effort and expenses incurred late in projects or even after implementation.

EG2.P.3 Privacy by Design and by Default should be strongly encouraged and can be incorporated in the methodologies of parties involved in Smart Grid development when personal data are involved. The application of this principle can effectively incorporate privacy measures into the development process and can improve control over the processing for the consumer.

2.1.4. Privacy Impact Assessment

87 Privacy Impact Assessments can help organisations to determine whether new technologies, information systems, services and initiatives or proposed programs and policies meet basic legal privacy requirements. It can help organisations to anticipate the impact on the public and may aid in anticipating the reaction of the public.

88 These analyses can prevent redesign and adaptation of systems, services or processes by considering the privacy impact of the development. The process is similar to a continuous risk management approach and includes planning, analysis and education activities. Depending on the implementation, the process can have the following core components:

a) Initial Analysis Phase.

b) Risk Assessment Phase.

89 A correctly performed PIA ensures that privacy principles and legislation are considered and that these are adhered to throughout the lifecycle of a new development. Where appropriate, a PIA can be used to determine where existing initiatives should undergo transformation or redesign. The method of performing a PIA can be described in a standard which can be adapted to the specific subject of Smart Grids.

90 Based on the current practice for RFID applications (25) a Privacy Impact Assessment can be either full scale or small scale. In the initial analysis phase a choice should be made for the type of PIA. In order for an organisation to make such a decision the nature and sensitivity of the data needs to be taken into account, as well as the nature and type of processing or stewardship of information it engages in, and the type of service provided to the customer. In order to be able to show accountability organisations should document the analysis.

91 If a full-scale PIA is needed the organisation needs to assess all relevant risks at a highly detailed level in order to be able to mitigate these risks. When impact to the public is considered less severe a simplified version of the PIA can be performed. The risk assessment phase of the PIA should identify the privacy risks associated with the service or application. This assessment should take place early on in the development process to be able to pro-actively manage and mitigate the risks. This approach can save time and cost of additions and changes made later on in the project. The process should at least:

a) describe the service or application;

b) identify how the service or application could harm privacy and assess the probability and impact of these risks;

c) list the different controls (technical as well as organisational controls that are in place or are planned to mitigate these risks;

d) document the resolution of the risks.

92 A documented and published PIA for an application can provide transparency for customers as well as provide accountability for service providers, and may save time and cost in implementation.

EG2.P.4 Member States to **Error! Not a valid bookmark self-reference.**

2.2. Data retention

93 Smart metering, by collecting and processing data on all electricity flows within the grid, is capable of contributing to ubiquitous surveillance of the energy consumers by collection of facts and details arising from consumption of electricity (cf. profiling). Depending on the actual technical design of a particular electricity grid, smart metering can have a profound negative impact on privacy. A suggestion that privacy is jeopardised may cause public trust to diminish unless proper compliance and strong enforcement are in place to convince the people. One of these aspects is the retention of data. These issues are of high importance for protection of privacy and personal data. Therefore, data retention for the purposes of smart metering needs an in depth analysis.

94 This chapter addresses these issues from an academic approach. The terminology used in this chapter needs to be considered; put simply, 'data retention' is a generic term that covers storing data (personal or any other type) for meeting various legal and business data archival requirements, as well as backup and historical purposes. Note that this term is much broader than the 'telecommunications data retention,' made famous by the 2006 Data Retention Directive. Therefore, the concept of data retention for the purposes of smart metering is a separate one and needs a deep analysis.

2.2.1. Analysis of the data retention purposes within smart metering

95 There are a seven reasons identified for the retention of personal and technical data within smart metering. Below a number of these reasons are listed. This list is non-exhaustive. Depending on future developments and desired functionality this list may be expanded.

2.2.1.1. Network Maintenance

96 The utilities need some data, both personal and technical in nature, that is required for standard network operation. For this kind of data, in many cases there is little reason for long term retention unless specified in local law or regulation – if it had not been used within a week, the data usually provides little benefit. Note that the 'week' is an approximation here – concrete numbers need to be verified with utilities, as they depend on the concrete procedures in network maintenance. Currently, there may also be specific legislation within Member States that dictates data retention.

97 For some long term maintenance functions, utilities need to store information for a longer period of time. In this case, unless specified in local law or regulation, the information could be aggregated, either over several users as to be large enough to ensure privacy, or by deriving very coarse grained information about a single customer (e.g. assigning one of ten customer profiles). Some cases (e.g. local legislation) may warrant the retention of more detailed data for a specific purpose.

98 One exception is if an extraordinary event happens – e.g. a blackout – in. In such a case some technical data needs to be kept for forensic analysis. This also includes fraud detection for example. In order to ensure that these data will not be abused, it is crucial to include rules on the burden of proof that could lie with the data

controller together with the notification of the data protection authorities in line with the principles of proportionality, among others.

99 However, taking into consideration the roles and responsibilities of various Smart Grid actors, it must be made clear that not all operators may need exactly the same data in order to maintain their (part of a) communications network or to fulfil their duties. Some operators will need detailed data and some might be satisfied on aggregated or anonymised data. Hence, special attention must be paid to those operators who process personal data (i.e. non-aggregated and not anonymised). The opinion of Art. 29 WP aims to clarify the responsibilities of the main actors involved.

2.2.1.2. Billing and payments (and related issues)

100 Certain data must be retained in order to compute the electricity bill. An estimate on the retention time is around a year, but depends on payment intervals. There is a difference among the Member States between the current practices on frequency when the customer is billed. To analyse a few current examples for analogue meters:

- in the UK, the customer is sent a hard-copy bill, either by email or by post, usually every three months or every month which tells them how much they must pay the energy company. This may be an estimate bill if the customer has not contacted the supplier with a meter reading or an accurate bill if they have or the supplier has visited since the last bill. The supplier must send a representative around to the house to physically read the gas and electricity meter every two years so that at least once every two years the customer will get an accurate bill;

- in Poland this system is quite similar, but the invoice is issued in a 6-months interval. Then the bill is divided in six equal instalments and paid monthly. Yet the customer is free to pay everything at once;

- in countries where billing interval is longer, the data are stored accordingly longer.

101 An analogue meter counts the electricity consumption since its launch. It retains 'summed up' data for – in fact – an unlimited period of time. A human intervention is needed to know the readings and to check their accuracy. However, for the smart metering, there is no need for human intervention. A customer is not required to send any data as this is done automatically. In case of a billing dispute, the latest measurement directive prevails which stipulates that even Smart Meters require to display consumption data as this is known today for standard meters.

102 Customers have a legal period in which they can challenge their bills (consumer redress). It is usually around 3-5 years from the 'due date' – date of payment required by the creditor, yet country dependent (i.e. statute of limitation for periodic payments). From the consumer point of view, data should be stored only for that period of time.

103 However, the question arises where these data should be stored. Data necessary for computing a bill can be stored both at the utility and customer side (the latter for instance for the purposes of transparency We would like to point out that there may be little reason to grant anyone but the customer access to this data. Thus, it should – depending on its purpose and national legislation – be stored locally, i.e. close to the customer (e.g. in the meter or a customer controlled third party service with strong access control and encryption).

104 It might be the utilities' duty to store all necessary information for conflict resolution, possibly in an encrypted form where the key is stored in the meter and only accessible to the owner of the meter (this can easily be done by means of public key cryptography). Also, a certain period should be stored in the meter and thus be easily accessible. This period might be one year (or 13 months) so that customers have access to their historic data, e.g. to better understand their energy use, or to decide, based on their energy consumption patterns, if an energy tariff is right for them should they wish to switch. If the detailed data, in case the customer could need to challenge their bill, is stored for a shorter period than the period in which the customer is allowed to challenge the bill, the customer must be warned about that fact. Hence, in case customers would like to challenge a bill later on, it is for them to prove any mistake done by a billing entity.

2.2.1.3. Taxation

105 Utilities need to maintain some financial data (i.e. on their income) for tax purposes for a specified time (tax records). It seems that tax record can sufficiently rely only on the top-line figures (e.g. the final sum of bills/invoices). This would not include detailed data on electricity consumption (e.g. the 15-min interval meter readings.) This data is, however, highly coarse grained – there is little reason to store more data than is already stored in the current setting. Regarding the length of retention period, the situation in particular Member States differs – e.g. 3 years in the United Kingdom, 5 years in Poland, 7 years in the Netherlands and 10 years in France.

106 Moreover, we take into consideration that customers could get a tax break (deduction) if they change their energy consumption patterns. Hence, certain data needs to be available to prove that. The statute of limitations (periods of prescription) for tax purposes is also between 3 and 5 years. In some countries, the method of calculation differs. I.e. it might not be counted from the date of bill, but from the end of tax year. In Europe, the tax year usually starts on 1 January (e.g. Poland) or on 1 April (e.g. in the UK) and includes 'whole' year. Then it might be almost 6 years. However, in this case the detailed data on energy consumption might be needed (i.e. that one uses energy after, let's say, 10 p.m. as this counts for tax breaks).

107 We have to take into consideration also the tax procedures. In a tax statement, a tax break can be claimed, but there is no need to provide evidence at this time. In case of control/audit, documents of proof have to be kept (until the elapse of the limitation period). Since it is solely the customer's interest to benefit from any tax deduction, these data should be stored locally (e.g. within a meter). Therefore, instead of the utility the customers need to keep the data if they want to benefit from a tax break. For example, customers might access metering data via a secure on-line platform and download a digitally signed document.

2.2.1.4. Added Value Services

108 Added value services are additional services, apart from energy supply, provided by the utility and/or third parties on a commercial basis. These are of high business-related importance for distributors and suppliers. They are capable of providing more benefits for all Smart Grids actors (e.g. energy savings), but also of too big an intrusion to private live.

109 At present, we do not know much exact examples of such services. Yet nobody can predict what market value for third parties can have the detailed data on energy consumption. Two simple examples can be given:

a) the optimisation of energy consumption (e.g. *'join the savings programme'*);

b) goods or services offered thy third parties: (e.g. *'since it is known that you do not use much electricity after 8 pm, go to the cinema half price'*).

110 In addition, the main value added services so fare (e.g. Microsoft Hohm or Google PowerMeter – analysis software installed on the consumer's computer) try to help save energy, but there is no direct financial incentive for the utilities (apart from having saved energy). However, this software is installed by customer and has no direct link to utility.

111 In order to satisfy the data protection principles, these services should be only optional. The customers – having been duly informed – need to explicitly agree to provide these data for this specific purpose. The use and collection of data and by whom needs to be clearly specified as well as the specific purpose and where the data will be stored. This agreement would also define the retention period, which should be justified by the specific use case and should be agreed upon by the responsible national data protection authority (DPA). While the data may be transferred using the Smart Grid system, we consider this data separate, and it should be governed by individual rules. In any case, this needs to be explicitly opted-in, i.e. for each added-value service separately.

112 The customer should have a right to withdraw consent easily, i.e. the customer's consent can be withdrawn at any time, free of charge, by simple means, without any reasoning, and suspended temporarily. Art. 9 of the e-Privacy Directive provides some guidance in this issue. It deals with the location data, yet it is useful for our purposes:

- Article 9 in fine gives the following rights to the end-user: 'The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.'

- Article 9(2) says: 'Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.'

2.2.1.5. Law enforcement

113 There are a number of points of interest for law enforcement (e.g. police, intelligence, tax and customs authorities) in smart metering's data retention. Here we are touching criminal law and thus the rules on due process (fair trial) and presumption of innocence must be observed.

114 Law enforcement agencies might be interested in access to records on energy consumption for investigation and crime prevention and anti-terror investigation purposes. In other words, any abnormality in energy consumption might serve as a clue for these purposes. Fiscal and social security authorities might also be interested, e.g. in determination whether the premises are used accordingly to the taxpayer's (or home occupant's) statements as e.g. their principal residence. Yet there seems little reason to process retained data of users that are not under explicit suspicion (i.e. data access and a request for data retention should require a judicial oversight).

115 A special case may be the application of the telecommunications data retention law, as telecommunication services may be used to transfer data. This data retention framework is currently under revision and is subject to a fierce debate. However, data automatically generated by the Smart Grid are of a very different nature of normal telecommunication data. If this framework applies, the mere fact of transmission of meter readings (hourly, daily, etc.) is to be recorded, but not the meter reading itself. (However, there is one exception, i.e. when a meter is designed in a way that it does not communicate if the readings are not much different from usual energy consumption. Then a mere fact of communication would indicate a difference.) Due to the fact that this is of little use for law enforcement, these records should be exempt from the telecommunications data retention regime.

116 Finally, there are certain grid-related crimes, e.g. sabotage or energy theft. Smart metering might also lead to identity theft, physical dangers (e.g. burglary, vandalism or stalking) or misuse of data. We maintain the position that similar rules as for grid maintenance and normal crime apply here – most grid related crimes can be detected on short term data (e.g. a day), and longer periods of measurement should only be allowed in case of a concrete suspicion upon judicial oversight.

117 Law enforcement is in principle a very legitimate purpose. But the question today is whether we should create data storage just to make more law enforcement possible compared with the current situation. This issue is very heavy debated because positive answer is actually leading to a society with a controlling infrastructure. However, we do not find any grounds for establishment of any special and separate data retention regime of energy (electricity) consumption details for the purposes of law enforcement. Current principles on crime investigation and evidence are sufficient.

118 A recent decision of the Constitutional Court in Karlsruhe on the German implementation of the Data Retention Directive[44] highlights the idea that even 'mere' data retention is not a trivial measure, but a measure that has concrete consequences on societies and thus must undergo a severe check. This also echoes the Strasbourg Court decision on the so-called Marper case[45], that decried the 'mere', but not time-limited, retention of personal data of acquitted or discharged people. This posture is particularly important in the face of a

[44]BVerfG, 2 March 2010, 1 BvR 256/08, at http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html
[45]S. & Marper v UK, 30562/04 and 30566/04

continuous shift in the nature of security and surveillance measures, heading towards systems based on the 'preventive' accumulation of commercial and non-commercial data of a great number of people[46].

2.2.1.6. Policy-Making

119 The state itself (as a regulator) might be interested in data retention for the policy-making purposes. It is a matter of energy security and production planning, among others. For example, stimulating actively the energy consumption in a given area (by awareness raising or tax breaks) might reduce energy demand in peak periods and allow consuming it in the time of availability. It is a matter also of ecology, carbon dioxide level objectives, etc. It is apparent that this purpose can be sufficiently fulfilled using only statistical data. It must be stressed that public policy objectives even sensitive ones must not override the fundamental rights of data subjects.

2.2.1.7. Profiling, red-lining and discrimination

120 The detailed data on electricity consumption might interest various commercial actors outside the electricity market, among others. The retained data are vital for making a customer's profile, as the creation of a profile highly depends on retained personal data. By 'profiling' we understand 'an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.' A 'profile' is 'a set of data characterising a category of individuals that is intended to be applied to an individual.'

121 Firstly, such profiling might lead to denial of services or increase their cost. This phenomenon is known as 'red-lining'. This term originates from the American banks in the 1970s that were marking a red line on a map to delineate the area – on a criterion of race, religion, ethnic origin and even lower income or any crime indication – where they would not make any business. This practice is unethical and now is prohibited by laws against discrimination, unfair commercial practices and undue influence, among others.

122 Secondly, even a simple and non-detailed profile of energy consumption might facilitate commission of certain types of crimes. For example, a fact that inhabitants usually go to work or school from 9 to 5 might make intrusion easier when they are not at home.

123 Profiling requires additional measures protecting personal data, e.g. specific and informed consent or focus on data minimisation. The use of intrusive profiling introduces the threat of misuse, by authorised as well as unauthorised parties (e.g. through data leaks). However, the actual scope of these threats depends on data security and access rights to these data. In particular, the conditions on transferring these data to certain types of third parties (e.g. banks) are of high importance here.

2.2.2. *Additional issues*

2.2.2.1. Data anonymisation and data aggregation

124 In 'classic' data retention, data that is anonymised is usually considered non-personal because the data subject can no longer be identified and thus is not affected by the data protection framework. However, it is almost impossible to ensure the full anonymisation of personal data and it is often possible to 're-identify' or 'de-anonymise' individuals hidden in anonymised data with astonishing ease (by using e.g. advanced algorithms or conjunction with other data sets). Therefore in some cases the means likely reasonably used for identification[47] would allow for the identification of the data subject and in consequence would lead to the processing of personal data which are subject to data protection principles.

125 To prove its inefficiency, let us focus on concrete example on anonymisation of data. Suppose you only get a 15-minute-reading of energy usage without any name, i.e. completely anonymous. What you see in this data is:

- the occupant is never going to work before 10, but working until very late, thus probably an academic;

[46] De Vries K., Bellanova R. & De Hert P. (2010) Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention, at http://www.ceps.eu/book/proportionality-overrides-unlimited-surveillance

[47] Recital 26 of Directive 95/46/EC.

- apart from Wednesdays where the occupant is getting up early (morning lecture);
- there is a lot of 2-3 day periods where the occupant is not at home – assuming we guessed right with academic, that is conferences.

126 Link these items with the public teaching schedules and conference speaker lists, and the occupant is pretty well identified.

127 Let us make also a reference to interesting research in the US that no data can be fully anonymised. The US Federal Trade Commission has recently acknowledged the distinction between personally identifiable and non-personally identifiable data is no longer meaningful in light of developments in profiling technology.

128 Concerning aggregation of personal data, there is no clear saying on how many persons one needs to aggregate on to protect individual data. This is also very context- and data dependent. Some research indicates that the minimum number of users is around 7 to 8, but in many circumstances it will be more. In case a meter is 'adjacent' to a household (i.e. majority of situations) we cannot say that we have any kind of data aggregation. There are simply too few inhabitants in such a household.

129 On the other hand, it is possible to have a smart meter that is able to 'tell' which exact device was used at a particular time. It is easy to build in and there is actually a lot of research in de-aggregating the readings. It is certainly easy to identify big devices like a washing machine, tea kettle, etc. When aggregating data it has to be ensured that individual households and devices cannot be recognized.

2.2.2.2. Storage of the data

130 Generally speaking, smart metering offers three possibilities of data storage: on operator(s)-side, on customer-side or both. The main difference between these options is whether data are stored using centralised or distributed (decentralised) method, or combination thereof.

131 Both solutions have their advantages and disadvantages. Advocates of centralised system usually point out: single storage place, easy access, transparency and low maintenance costs, among others. Opponents argue that it threatens security, facilitates abuse and it is not proportionate (i.e. the same results could be obtained using less invasive methods).

132 Taking into consideration the characteristics of smart metering, all three above mentioned options apply. It is our opinion that personal data are the best protected if stored at the customer's side to the highest possible extent compatible with national law.

2.2.2.3. Data mobility

133 One special case in the Smart Grids is that customers are rather mobile, i.e. they change providers, third party services, and dwellings. It has to be ensured that the data stays linked to the customer or is deleted altogether. This requires a cross-organisational and cross-device approach, which needs an effective regulatory framework as well as standardised interface for secure information transmission (end-to-end security).

134 In case the customer changes a location, the data from previous meter must be erased and transferred to a new location. If a customer changes only a provider and not the location, the data should be transferred to the new provider.

2.2.2.4. Access to the stored data

135 The following parties may gain access to the stored data:

a) Consumers: it is one of the basic rights of data subjects to access their personal data. The consumer must be the only person to have unlimited access to both the detailed meter readings (current) and historic data. These data should be accessed by simple means, at any time and free of charge. Consumers should be able to authorise anyone to access these data.

b) Utilities: consistent with the previous, utilities must access certain data in order to maintain the network. However, the scope of this access right is different than the consumer's, i.e. is narrower. In case the utility is required to retain data, it must keep it protected, e.g.by encryption or access controls.

c) Third parties: it can be expected that some customer data will be processed by third parties, to whom different jurisdiction applies. It is vital that those third parties seek explicit customer consent to use the data and are bound by the same data retention rules as the original data controller. The current legal framework provides that personal data can be transferred to third countries (i.e. outside EU/EEA) only if they provide adequate level of protection (or upon one of the exceptions provided in the Data Protection Directive). Hence, if the third party resides in a country where such rules cannot efficiently be enforced, no data relating to individual should be accessible to those parties. Special care has to be taken if approaches like cloud computing are used, where data handling is often not transparent. In case of dispute the law applicable should be the law of the residence of the consumer.

2.2.2.5. Consumer empowerment

136 In many cases, consumers are overwhelmed with information they need to agree to. They often sign away control of their data, as picking out the default option is a typical human characteristic (behavioural economics). In addition, privacy notices aim namely to comply with legal obligations rather than inform the consumer, while in most cases they fail to provide consumers with information on those issues that matter the most, such as what data are to be collected, by whom, for what purposes, for how long, etc.

137 Moreover, consumers need to properly understand and engage with smart meters. This is particularly important to achieve the behaviour change needed to deliver the energy efficiency savings. Therefore, when smart meters are installed, consumers should be provided with information on their energy consumption as well as on their historical consumption free of charge.

138 If customer consent is needed, it has to be made sure that the conditions they agree to be communicated in such a way that it can be clearly understood by all consumers, including those who are vulnerable. Therefore, when a customer's consent is needed, it should be ensured that such consent is meaningful so that consumer understands what it is they are agreeing to.

139 Moreover, in order to make sure the customer is properly informed about processing of the personal data in smart metering, a company collecting personal data must ensure that they communicate in a clear and intelligible way to customer. This should be directly communicated to the consumer. It would serve these purposes if such information must be printed out in language(s) understood by the consumer and consist – at least – of:

- name of and the contact details to the data controller and processor,
- a brief list of consumer rights regarding processing personal data,
- information what types of data are retained and how long,
- how to file a complaint regarding billing and processing personal data,
- information about available means of ADR and other means of redress.

EG2.P.5 Given the variety of data storage purposes within smart metering, a single data retention period cannot be concluded. In other words, each such purpose has its own characteristics and a specific data retention period. Next, we cannot interfere with national criminal (tax) laws and civil procedures.

EG2.P.6 EG2 recommends Member States to perform an analysis in order to determine to which extent utilities need to retain personal data (i.e. neither non-aggregated nor anonymised) to be able to maintain and operate the electrical grid and perform billing.

EG2.P.7 Following EG2.P.6, the following principles should apply for the purpose of data retention: (a) data minimisation – i.e. the scope and length of both (i) data collection and (ii) data retention shall in any case not exceed what is necessary to achieve specific and lawful purpose. (b) transparency – i.e. who, when and in what circumstances collects, processes and retains personal data for what purposes, and what data and where is stored; (c) empowerment of the consumer – i.e. safeguarding consumer's rights (including information). In case the personal data are to be collected and processed – to ensure full compliance with the data protection Directive, namely the principles of data minimisation (Art. 6(b)-(c) of the 1995 Data Protection Directive). A recommendation on specific retention periods is shown in section 2.2.2.6.

2.2.2.6. Examples regarding data storage

140 Concerning the scope and length of data retention and entities involved, the following periods could be considered:

Purpose	Scope	Length	Kept by
Network maintenance	Personal/anonymised/aggregated	strictly necessary / national law	Utility
Billing and payments	summed up usage	around 12-13 months / national law	Utility and energy market supplier
Billing complaints	detailed personal data	national law	consumer
Taxation – tax records	summed up usage	national law	utility
Taxation – tax breaks	detailed personal data		consumer
Value added services	upon consent	upon consent	any interested
Policy making	anonymised/aggregated	unlimited	public authorities

141 Regarding law enforcement purposes, all these conditions would be decided on a case-to-case basis in accordance with national law. Rules on fair trial must be duly observed. It is rather a question of conditions on access to any retained data by any of law enforcement bodies. We cannot interfere with that.

142 Profiling shares a lot of similarities with law enforcement purposes, i.e. it is a question who and when can have access to what data. Generally speaking, negative effects of profiling must be avoided as it leads to discrimination, information misuse, fraud or security risks, among others. It is also a question of data security.

143 The following issues need some explanation:

a) utilities – in most cases – need only granulated data for network maintenance for a very limited period of time (however cf. also point *h*);

b) detailed data on electricity consumption should be retained as close to the customer as possible, e.g. in a meter (to the highest possible extent)

c) it should be the utility's responsibility to keep protected records of their customer's energy consumption if the latter wishes to challenge his/her electricity bill, for a limited period of time (possibly based on national legislation); upon elapse of such period of time, it would be the customer's sole responsibility to keep these data for this purpose;

d) it should be only the customer's responsibility to receive from the utility and then to keep records of his/her energy consumption if s/he wishes to benefit from a tax break (deduction);

e) any added value services (cf. 2.2.1.4) can be provided only upon a separate, prior, informed and explicit consent of the customer; due observance of data minimisation principle must be ensured; such a consent could be withdrawn at any time, by simple means, without reasoning and free of charge;

f) personal data gathered from smart metering must always follow the customer in case of a change of localisation or a provider; if not, they must be erased;

g) in addition, we ask for an analysis in order to determine to which extent utilities need to retain personal data (i.e. non-aggregated nor anonymised) in order to be able to maintain the electrical grid.

2.2.3. Data breach notification

144 Article 13a of the recently changed E-Privacy Directive requires notification of security / data breaches in telecommunication networks. In some cases, the communication part of Smart Grids may be carried by public telecommunication providers causing the obligation for data breaches to be reported to ENISA and national authorities. Moreover, the European Commission as stated in the communication on the revision of the Data Protection framework (26) has the intent to extend this legal requirement to all sectors. The development of Smart Grid applications and logging better shall take into account the probability that Smart Grids need to implement such a legal requirement.

145 The following issues may develop in the future and should be considered. Further research is needed to identify risk so that necessary and appropriate additional measures can be considered:

- Upgradability: the smart-grid is a highly complex system with likely changing requirements, contexts, and components. Furthermore, it is a system that (ideally) always be live, has components that will remain unaltered for decades, and may be subject to advanced attacks. This puts special requirements to the upgradability of devices and components - upgrades have to work in a life system, need to implement different trust models (for example, certified units cannot be remotely upgraded), and may have to be pushed through extremely low bandwidth communication lines.

- Dependability and Fail Safes: most critical control systems are designed in a fail-safe way, i.e., failure of individual components will push the system into a state that causes the least damage – e.g., a forced shutdown to assure nothing explodes. While a lot of work has been performed on dependability of critical systems, none have ever experienced this scale.
  In addition, there is insufficient experience in the areas bordering security, dependability, and control systems; most safety systems will not survive the interference of an active attacker, while most security systems will be a dangerous threat to availability.

- Meter-End Device Interaction: at the periphery of the Smart Grid, we can expect cheap devices with restricted user interfaces. Those devices need to be integrated without introducing a security loophole, and while maintaining usability aspects.

- Smart Grid meets the Cloud: given that the Smart Grid might add new data processing capabilities, it is not unlikely that some Smart Grid functions will be externalised towards cloud providers. This does add new legal and technical challenges, as cloud systems are not designed for highly reliable systems, and data and computation may freely float between various legislative domains.

- Forensics and Intrusion detection: the smart gird is a highly distributed system, which makes it hard to detect corrupted components, and to start a forensic investigation to figure out what went wrong – in the past, such investigations have failed for minor issues as the lack of synchronised time to determine the order in which events happened. A special issue here is reliable remote measurement to be able to test remote devices in a reliable way without adding extra hardware or to use immense bandwidth.

- Domestic Privacy and confidentiality: An item completely unaddressed so far is the issue of domestic privacy, where several parties share a meter or have access to other peoples' meters – examples are a family setting, shared flats, landlord-tenant, or big apartment blocks with a centralised meter location.

2.3. Privacy certification / EuroPrise

146 Organisations will be concerned with whether the personal data they process is handled in accordance with data protection principles and whether the organisation has an adequate and effective Personal Data Protection

system in place. Assurance on these matters can be provided by a data protection audit. A data protection audit can help the organisation to:

a) identify non-compliance issues and/or to detect weaknesses in its own data processing management structure;

b) ensure and/or maintain compliance with relevant data protection requirements.

147 A data protection audit may also contribute to avoiding breaches of statutory obligations (breaches which may result in sanctions, without excluding other obscure effects for the company's reputation and long term welfare). In addition, for some organisations the data protection audit is an important means of demonstrating compliance with data protection rules (e.g. via a trusted third party opinion and/or a certificate of compliance and/or a letter of comfort). A positive outcome from an audit can be used by an organisation as a marketing tool to gain a business advantage over its competitors. It is important to ensure strict criteria for certification is established.

148 A privacy certificate of compliance could be one way for organisations to show to data subjects that they deal with the protection of their personal data with due care. Interest groups can also urge an organisation's management to obtain a privacy certificate. The privacy certificate must be formulated clearly, unambiguously and be socially acceptable.

149 Achieving a privacy certificates can be a large and complex undertaking. It is therefore necessary to formulate requirements with respect to the meaning and contents of the certificate, and to formulate requirements on the expertise of those issuing the certificate. The requirements that the processing of personal data must comply with can be further detailed in a national certification scheme. The requirements for the auditor and the method by which the privacy audit is carried out need to be shown in the accreditation scheme.

150 An example of certification that can be applied is the certification provided by EuroPrise. This is a dedicated, independent organisation, certifying the privacy compliance of IT products and IT-based services against the European data protection regulation. The privacy certificate aims to facilitate an increase of market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing Technologies and finally an increase of trust in IT.

EG2.P.8 The use of privacy certification schemes should be encouraged by Member States. When provided by independent parties these schemes can provide transparency and trust to customers as well as for the actors responsible for the Smart Grid. Further research to determine which certification scheme, strict criteria and structure should be used is necessary.

2.3.1. DPAs and Smart Metering legislation

151 In order to identify and produce a set of regulatory recommendations to ensure EU-wide consistent and effective implementation of Smart Grids, while achieving the expected Smart Grids' benefits for the network users without negative consequences, and to assess how personal data in relation to Smart Grids and smart metering are dealt with in these states EG2 has asked a number of questions to the Member States through the Article 29 Working Party.

152 Not all DPAs were completely involved in the legislative process during preparation and implementation for Smart Grid/metering. Usually Privacy Impact Assessments (PIA) or risk assessments were not performed and Data Protection Authorities (DPA) were not always included in the drafting of legislation specific to Smart Grid / metering purposes. It is recommended to include DPAs in the legislative process in the eleven states that have not yet implemented directive EC2006/32 into legislation. It is also advised to perform PIAs on the infrastructure architectures, both existing and planned. The responsibility for performing these PIAs should not necessarily lie with the DPAs, but may be requested from the intended (joint) controllers of the data and approved by the DPA or can be performed by the legislator. As a matter of fact, according to Art. 20 of Directive 95/46/EC prior checking is required for processing operations which are likely to present specific risks to the rights and freedoms of data subjects and these operations shall be checked prior to the start of the operation.

153 From answers to the questionnaire on Smart Grids (appendix H) it shows that legal bases for processing Smart Grid data are not always clearly defined. The legitimate purpose for use of data varies and may be found in informed consent or in contractual or legislative obligation. Responses to questions to DPAs in different Member States indicate that the legitimate purpose depends on the use and nature of the data. In general, billing may be part of contractual or legislative obligations, while additional uses require the consent of the subject. This also reflects on who is considered to be the controller of the data. In a structure where the billing party differs from the collecting party it may not always be clear who is considered the controller of the data.

EG2.P.9 The opinions on the protection of personal data from Smart Grids differ widely between Data Protection Authorities (DPAs). In order to be able to adequately protect consumer rights and enable the effective use of Smart Grids DPAs need to be involved in the process, but also need to be able to apply a consistent set of responsibilities, definitions and principles. DPAs should be involved in these steps, but the actors should be able to show accountability themselves. Accountability should enhance not replace the obligations of the data controllers to comply with data protection legislation.

2.4. Privacy and data protection challenges for Smart Metering

154 Smart metering promises to increase efficiency, optimise supply and demand, reduce energy losses, minimise the risk of energy theft, integrate renewable generation sources (e.g. wind) and raise customer awareness of energy usage and costs, among others. However, smart metering also affects a number of fundamental rights, in particular the right to privacy, the right to protect personal data and the principle of non-discrimination.

155 Protection of these rights and principles strongly interests various stakeholders. It is worth to mention here that the European Parliament currently considers drafting a report on energy infrastructure priorities for 2020. In its proposal, the Parliament would call for 'rules concerning privacy and data protection to be established in accordance with existing EU law'[48].

156 The following can be concluded in the field of privacy in Smart Metering:

- Smart metering can pose considerable challenges to privacy and data protection. Therefore the least intrusive options for smart metering are in principle to be preferred. In any option special safeguards for the data subject are needed.
- The exact response to these challenges and the exact choice of safeguards is highly dependent on the technical design (functionalities) of a given smart metering solution. All solutions must comply with existing legislation of data protection and privacy.
- The current EU regulatory framework for smart metering, namely the Energy Internal Market Directive and the Measuring Instruments Directive, insufficiently regulates the protection of privacy and personal data, and therefore the Framework Directive on protection of personal data should be applicable.
- Each smart metering solution requires the assessment whether its interference with the right to protection of personal data and privacy complies with the legislation and respects the principles of legality, necessity and legitimacy, and whether it is proportionate to the aim pursued.
- Each smart metering solution needs to respect the general EU data protection principles. There is a need for tailoring them down to a more concrete regulatory level for smart metering options that rely on the processing of personal data. Regulation should make clear who is data processors and who is data controllers and their respective responsibilities,[49] should apply the application of the data minimisation principle, and should clarify the length and scope of data retention, the scope and exercise of the data

[48] European Parliament, Committee on Industry, Research and Energy (Rapporteur: Francisco Sosa Wagner), *Draft Report on energy infrastructure priorities for 2020 and beyond* (2011/2034(INI)), para 22, at http://www.europarl.europa.eu/oeil/file.jsp?id=5898472.

[49] Cf opinion 12/2011 Art. 29 WP

subject's rights, the legitimate goals pursued and the measures taken to safeguard security and confidentiality of data processing.

2.4.1. Smart metering options

157 First and foremost, there is no single 'option' of smart metering. In other words, what a smart meter within an electrical grid can offer, it highly depends on its functionalities chosen by the operator and/or regulator. Among these options, the most interesting from the privacy point of view, are:

- the (possible) compulsory use;
- the interval of meter readings;
- the scope and length of storage (retention) of data concerning the energy consumption;
- the access to such data;
- the remote control by the operator.

158 The current EU framework for Smart Grids does not set forth any legal requirements as to the functionalities of smart metering.

2.4.2. Current EU legal basis for smart metering (Smart Grids)

159 Currently, in the EU, there are two main legal bases for smart metering:

- Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (Energy Internal Market Directive);
- Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments (Measuring Instrument Directive).

2.4.2.1. Energy Internal Market Directive (EIMD)

160 The former instrument is a part of the Third Energy Package (2009). The EU internal market in electricity aims at, inter alia, achieving efficiency gains, competitive prices, higher standards of service and security of supply. The Package encourages a long-term modernisation of electrical grids in Europe, among others.

161 From the policy-making point of view, regarding smart metering, this Directive stipulates that:

- Member States 'should encourage the modernisation of distribution networks, such as through the introduction of Smart Grids, which should be built in a way that encourages decentralised generation and energy efficiency' (Recital 27);
- 'In order to promote energy efficiency, Member States … shall strongly recommend that electricity undertakings optimise the use of electricity, for example by … introducing intelligent metering systems or Smart Grids, where appropriate' (Art. 3(11));
- 'It should be possible to base the introduction of intelligent metering systems on an economic assessment' (Recital 55);
- Member States 'shall ensure the implementation of intelligent metering systems that shall assist the active participation of consumers in the electricity supply market. The implementation … may be subject to an economic assessment of all the long-term costs and benefits to the market and the individual consumer … Such assessment shall take place by 3 September 2012 … Where roll-out of smart meters is assessed positively, at least 80% of consumers shall be equipped with intelligent metering systems by 2020' (Annex 1, paragraph 2);

162 It contains also a number provision concerning processing the personal data within electrical meters. Yet these provisions focus on the objective and transparent consumption data:

- the regulatory authority shall ensure 'access to customer consumption data' (Article 37(1)(p));
- the consumer shall 'have at their disposal their consumption data, and shall be able to, by explicit agreement and free of charge, give any registered supply undertaking access to its metering data' (Annex I, paragraph 1(h));
- the consumer shall be 'properly informed of actual electricity consumption and costs frequently enough to enable them to regulate their own electricity consumption. That information shall be given by using a sufficient time frame, which takes account of the capability of customer's metering equipment and the electricity product in question. Due account shall be taken of the cost-efficiency of such measures' (Annex I, paragraph 1(i);
- the consumer shall have a right to a contract with their electricity service provider that 'specifies information relating to consumer rights, including on the complaint handling and all of the information referred to in this point, clearly communicated through billing or the electricity undertaking's web site' (Annex I, paragraph 1(a)).

163 No additional costs shall be charged to the consumer for any of the above mentioned services.

2.4.2.2. Measuring Instrument Directive (MID)

164 This directive applies to the measuring instruments like water, gas, electricity or heat meters. Firstly, it establishes the essential requirements that these instruments will have to satisfy and the conformity assessment that they have to undergo prior to their placing on the market and putting into use. Secondly, it provides that Member States shall not impede the placing on the market and putting into use of any measuring instrument that carries the CE conformity marking and supplementary metrology marking.

165 Important for our purposes is a fact that this Directive implicitly prescribes the 'minimum' period of the data retention within an electricity meter: 'In the event of loss of electricity in the circuit, the amounts of electrical energy measured shall remain available for reading during a period of at least 4 months' (Annex MI-003, paragraph 5(3)).

2.4.3. Smart metering and privacy

2.4.3.1. Privacy testing of smart metering: overview

166 Some smart metering options pose considerable challenges to privacy (e.g. surveillance, profiling, abuse of information, threats to data security, etc.). Art. 8(2) of ECHR and the case-law of ECtHR set forth the requirements to assess a legitimate interference with the right to privacy (i.e. legality, necessity, legitimacy and proportionality)[50]. While it is quite easy to enact the Smart Grids legal framework (i.e. to fulfil the criterion of legality), it is much more difficult to assess whether its interference with privacy can be justified (i.e. necessity, legitimacy and proportionality).

167 The scope of the said interference with privacy and data protection depends on two factors:

- a regulatory framework for smart metering;
- a given smart metering solution.

168 Therefore, such interference can be found justified if both these factors prove to:

- have a firm, clear, specific and foreseeable legal basis, enacted in a statute (legality);

[50] Cf. chapter 1.1.2.

- be necessary in a democratic society (necessity);
- serve at least one of the certain public interests (legitimacy);
- be designed in a way that its interference with privacy is proportionate.

169 In addition, a privacy impact assessment (PIA) is nowadays considered as a good means to address the information society challenges. A PIA may be defined as a systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and finding ways to mitigate or avoid any adverse effects.

2.4.3.2. Legality

170 The first element of the privacy test is the criterion of legality, i.e. any interference must be prescribed by law ('in accordance with the law'). The ECtHR ruled that this phrase includes[51]:

- 'A norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail; however, experience shows that absolute precision is unattainable and the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are flexible.
- The phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law; it thus implies that there must be a measure of protection in domestic law against arbitrary interferences by public authorities (...).
- A law which confers a discretion is not in itself inconsistent with the requirement of foreseeability, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (...)'.

171 Concerning the current provisions of the EU smart metering framework (see para 3), it is our opinion that privacy and data protection is insufficiently regulated. Therefore, it is important to clarify the application of the framework Directive on data protection and e-privacy on smart metering. We have analysed the following:

- these instruments strongly focus on the organisation of the internal energy market, technical issues and consumer rights;
- they do not focus on privacy and data protection;
- they do not set forth any legal requirements as to the functionalities (options) of smart metering thus allowing free choice for national regulators and operator;
- both these Directives are silent about privacy;
- regarding processing of personal data, these Directives only mention in a very brief way:
  - access and information rights (EIMD, Art. 37(1)(p): 'ensuring access to customer consumption data'),
  - explicit consent for value added services (EIMD, Annex I, para 1(h): consumer 'shall be able to, by explicit agreement and free of charge, give any registered supply undertaking access to its metering data', and

[51] ECtHR, *Olsson v Sweden*, 10465/83, § 61.

  - data retention period (implicitly) (MID, Annex MI-003, para 5(3): readings 'shall remain available for reading during a period of at least 4 months');

- these provisions are not sufficiently precise nor clear;
- they do not exhaust all data protection principles – the EU data protection framework is very complex and a number of substantial issues is missing (e.g. concept of data controller, data retention or legal basis for processing personal data).

172 Moreover, there is a risk of insufficient protection of privacy rights due to fragmentised legislation. The right to privacy and protection of personal data are much better safeguarded when they are of a uniform nature throughout the EU. A negative experience of the regulatory framework on the identity documents with biometric data, where all provisions regarding fundamental rights were left for the Member States, should be avoided.

2.4.3.3. Necessity and proportionality

173 'According to the Court's established case-law, the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued; in determining whether an interference is 'necessary in a democratic society', the Court will take into account that a margin of appreciation is left to the Contracting States.'[52]

174 The scope of privacy covers a wide range of issues. One of them is the concept of free choice as to one's private life. From the standpoint of privacy, freedom of choice between a smart or a traditional meters is important. Compulsory use of smart meters deprives the user from their free choice. The option for a traditional meter could, after all, provide assurances against breach of privacy.[53]

175 For example, in the Netherlands, their initial Smart Grid proposal (2008) was found by legal scholars 'not necessary in a democratic society' and thus violating the right to privacy. The following were questioned:

- the 15-minutes/ hourly/daily readings of a smart meter;
- a compulsory use thereof;
- remote switching function;
- a signalling function for combating fraud[54].

176 In order to fulfil the criteria of necessity and proportionality, the following questions are useful:

- is (a given solution of) smart metering necessary in a democratic society?
- is this interference proportionate to the aims pursued?
- is there any less intrusive (onerous) solution?

2.4.3.4. Legitimacy

177 Art. 8(2) of the ECHR lists the following legitimate criteria of interference with the right to privacy:

- 'national security, public safety, the economic well-being of the country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others.'

---

[52] ECtHR, *Olsson v Sweden*, 10465/83, § 67.
[53] Cuijpers C. & Koops B.-J. (2008) *The 'smart meters' bill: a privacy test based on article 8 of the ECHR. Study commissioned by the Dutch Consumers' Association*, Tilburg Institute for Law, Technology, and Society (TILT), unpublished, p. 10.
[54] Cuijpers C. & Koops B.-J. (2008), *op. cit.* p. 36.

178 The criterion of the „economic well-being of the country' seems to play the most important role. In order to answer whether smart metering contributes to this goal, the following questions might be useful:

- whether they contribute to energy savings at the consumer level;
- whether they contribute to an efficient, reliable, fair and competitive energy market;
- whether they increase the usage of renewable sources of energy;
- whether they increase energy efficiency at the producer level.

179 The criteria of 'national security' and 'public safety' play here some auxiliary role. It is apparent that a well-functioning energy market is vital for national economy and security. It must be proved that smart metering contributes also to this goal.

180 As a result, before the deployment of smart metering, it must be assessed whether a given smart metering solution is serving any of the above mentioned purposes. However, an interference with the right to privacy can be found justified only if one of these criterion is satisfied, i.e. 'economic well-being' only. It is edifying that the Energy Internal Market Directive already requires the economic assessment of smart metering (cf. e.g. Recital 55).

181 It is our opinion that the legislator (and operator(s), if applicable) must provide sufficient evidence that the interference with privacy made by smart metering is a legitimate one.

2.4.3.5. Requirements set forth by CFR

182 Art. 52(1) of the Charter of the Fundamental Rights (CFR) contains a general provision on legitimate interference with any of the rights it provides for. This provision reads: 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'

183 While there is no difference with the ECHR regarding the criteria of legality, necessity, legitimacy and proportionality, the CFR additionally requires that any such interference must 'respect the essence of those rights and freedoms.'

2.4.3.6. Non-compliance with conditions of privacy limitation

184 This sub-chapter aims at listing possible consequences of non-compliance with the privacy limitation criteria set forth predominantly by ECHR and CFR. It overviews both national and supranational level (i.e. the EU), as non-compliance can occur at both these levels. For the sake of clarity, note two points. First, that these deliberations are of extremely general nature. Second, that they could be easily applied to limitation of majority of fundamental right.

1. Substantive issues

a. Uniform application

185 *Privacy is a const*itutional standard in contemporary European democracies. It is considered as a "first" generation human right, i.e. a political freedom. Both the ECHR and CFR are of uniform application throughout their territorial scope, yet the states enjoy certain margin of appreciation. The ECtHR and ECJ observe uniform application of the Convention and of the Charter, respectively (see *infra*). Thus the concept of privacy could be regarded as being of uniform nature within each of these systems.

186 In consequence, national laws should ensure conformity with this uniform standard, especially in case of a lack of EU-wide regulatory scheme for Smart Grids (metering) or before such a scheme enters into force. Moreover, the EU's respect for fundamental rights and an explicit reference to ECHR in Art. 6 of the TEU obliges also the Union to observe this standard.

b. Supremacy of the EU law

187 *By virtue of the EU Tr*eaties, any EU regulatory framework overrides national legislation in case of conflict of norms. The EU law may not be revoked or amended by national law and that it takes precedence over national law if the two conflict. As the ECJ pointed out, "*the law stemming from the Treaty, an independent source of law, could not, because of its special and original nature, be overridden by domestic legal provisions, however framed*" (*Costa v. ENEL*, case no. 6/64).

c. Obligation to protect fundamental rights

188 *It shall suffice to mention here that t*he ECtHR on a numerous occasions held that a state has a positive obligation to take measures to ensure privacy, even in the sphere of relations between individuals (*X and Y v. the Netherlands*, application no. 8978/80, § 23). This standard can be applied to other rights as well. In particular, states need to take measures that make the exercise of fundamental rights possible (*Marckx v.* Belgium, application no. 6833/74, § 31), *and* need to introduce specific provisions for prevention and/or punishment of acts of individuals who ignore or violate basic rights or obligations (*X and Y v. the Netherlands*, § 23).

d. Fundamental rights' limitation criteria

189 *As it has been already mentioned, the* criteria of privacy limitation (*hereinafter*: limitation criteria) laid down in Art. 8(2) of ECHR are cumulative. The same goes for Arts. 7 and 52(1) of CFR, but the latter adds also that any limitation must "*respect the essence of* […] *rights and freedoms*." Put simply, any legal instrument regulating Smart Grids (metering) that interferes with privacy must fulfil all of them, i.e. legality, necessity (and proportionality) and legitimacy. (When it comes to legitimacy, it suffices if the interference in question satisfies at least one of its criteria, e.g. economic well being of the country.)

190 For example, the mere fact that national law prescribes conditions for interference with privacy usually *does* fulfil the criterion of *legality*. However, it *does not* necessarily mean that the said national law is in conformity with the rest of limitation criteria. Under no condition the fulfilment only of the legality criterion could justify interference with a fundamental right.

191 Another example could be given. When it comes to the criterion of legitimacy, it is difficult to justify supremacy of economic efficiency over privacy. Both notions are legitimate, yet their "weight" is different. There is a need to find a right balance between these two concurring notions. The ECtHR has dealt with such a problem e.g. in the case of *Hatton et al. v. the UK* (application no. 36022/97, *cf.* §§ 102ff). The applicants complained about night flights at Heathrow airport in London, in particular about the level of noise. The Court found that the authorities who had regulated this issue did not overstep their margin of appreciation by failing to strike a fair balance. In consequence, the Court held there was no violation of Art. 8.

192 In a number of cases the Strasbourg Court dealt with the question of reconciliation of concurring interests, especially in *Fägerskiöld v. Sweden* (application no. 37664/04; decision on inadmissibility) or in *Moreno Gómez v. Spain* (application no. 4143/02). In the former, the Court took into consideration that "*wind turbine is in the general interest as it is an environmentally friendly source of energy which contributes to the sustainable development of natural resources*" and found the alleged interference not sufficiently severe and thus proportionate. In the latter, the Court analysed noise pollution and underlined a need for a "*fair balance*" between "*the competing interests of the individual and of the community as a whole*" and found violation of Art. 8. These cases serve as guidance.

2. Procedural issues

193 In Europe, individuals benefit from an extensive system of fundamental rights protection. National constitutional or supreme courts (tribunals), ECtHR or ECJ might examine a piece of legislation against compliance with privacy limitation criteria set forth in a respective instrument. However, the nature of these courts is different.

a. Abstract judicial review

194 *National constitutional* or supreme courts (tribunals) are usually allowed to hear constitutional complaints filled in by individuals, public authorities, political parties or ombudsmen, among others. Generally, they are in

position to ultimately declare the piece of legislation in question void (with a retrospective effect or from the date of the judgement, or from a specific date in the future).

195 The spectrum of relevant legal action types that the Luxembourg Court can hear includes preliminary rulings (Art. 267 TFEU) and actions for annulment (Art. 263 TFEU). In case of the former, national courts can seek guidance in application of the EU law. These rulings have a precedent character. In case of the latter, the Member States and the EU institutions might lodge actions against all EU measures likely to affect their interests. Here, the Court can declare a piece of EU legislation void.

b. Individual complaints

196 *When it comes to the* Strasbourg Court, it hears complaints of the individuals against the State. The following are the admissibility criteria: (1) all national remedies have been exhausted and (2) complaint is lodged within 6 moths from the final decision against the victim of the claimed fundamental right(s) violation. The case is inadmissible if (1) it is anonymous, (2) is substantially the same as a matter that has been already decided by the Court, or (3) the applicant has not suffered a significant disadvantage. (The last condition is a novelty effective from 2010.)

197 If the Court finds violation, it awards damages for the victim (both pecuniary, i.e. suffered loss, and non-pecuniary damages, e.g. compensation). However, the Strasbourg Court – not being a constitutional court – is not in a position to declare a piece of national legislation void.

198 Note also that the EU is currently negotiating its accession to the ECHR. In result, individuals would be allowed to file a case against EU institutions, agencies, bodies, etc. for the alleged violation of the Convention.

199 In addition, national courts usually could award damages for violation of fundamental rights if such a violation results from the behaviour of public authorities, e.g. if a piece of legislation has been found unconstitutional. Moreover, national criminal codes penalise crimes against protection of personal data, among others.

200 The excerpt below summarises the possible consequences of non-compliance with ECHR or CFR, in particular with the privacy limitations:

Possible consequences of non-compliance with privacy limitations

1) Abstract judicial review
    a) National supreme or constitutional courts (tribunals) – **annulment**
    b) ECJ (Luxembourg Court)
        - action for annulment – **annulment**
        - preliminary ruling – **compensation** by national court involved

2) Individual complaint
    a) National courts
        - civil action – **compensation**
        - criminal action – **penalty**
    b) ECtHR (Strasbourg Court) – **compensation**

Conclusion

201 ECtHR emphasised that states are obliged to protect fundamental rights. Various senior courts have examined the privacy limitation criteria extensively. Non-compliance with this criteria, risks judicial review that could result in immediate repeal of the examined legislation or compensation. In rare cases, criminal law could also apply. Individuals, among others, are entitled to file a complaint. In result, non-compliance with privacy limitation criteria might have an adverse effect on Smart Grids deployment in a given electricity market. Both enactment of a regulatory framework and a practice that respect these limitation criteria will minimise such a risk.

EG2.P.10. Privacy is a constitutional standard in contemporary European democracies. Non-compliance with privacy limitation criteria might have an adverse effect on Smart Grids deployment in a given electricity market. It is recommended that both a regulatory framework is enacted and a practice that respects these limitation criteria is introduced. We recommend that interference should be justified on a case-to-case basis, assessing legality, necessity, legitimacy, proportionality.

2.4.4. Smart metering and data protection

202 Put very simply, the EU data protection framework is based on the principles of fairness, lawfulness, minimisation, quality, legality and security. It is apparent that smart metering interferes with these values. These principles proved to be sufficiently clear and satisfactory, but there is a need for tailoring them down to a more concrete regulatory level.

203 We have observed the following data protection challenges, each of equal importance:

- classification of data processed within smart metering as personal and non-personal data;
- distinction between the data processors and controllers;
- application of the data minimisation principle;
- length and scope of data storage;
- scope and exercise of the data subject's rights;
- legal basis for processing;
- enforcement
- security and confidentiality of data processing.

204 Firstly, it must be clear whether and what data processed for smart metering are the personal data and thus whether the EU data protection framework apply. Two types of data are processed within smart metering:

- personal data – definition in accordance with the Data Protection Directive;
- technical data – any data needed for maintenance of the grid.

205 These concepts overlap (i.e. technical data could be also personal data). However, majority of the categories of data processed within smart metering somehow refers to an identified or identifiable person. Yet it is our opinion that – whenever possible – Smart Grids operation should be based on non-identifiable data.

206 Secondly, there are various actors within Smart Grids, e.g. a range of grid operators (transmission- (TSO) and distribution system operators (DSO) or energy producers). Hence the distinction between data controller and data processor might be blurred. This distinction is crucial as it determines who is responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective national DPA can operate. Note that this distinction based on a factual rather than a formal analysis[55]. The Article 29 Data Protection Working Party has provided an opinion on the different roles, with the caveat that these may be specific to the situation in the different Member States or the nature of the different markets (20).

207 It might also happen that the identity of the controller is decided where there are 'multiple actors interacting in the processing of personal data' (i.e. 'joint control'). The assessment of this joint control should mirror the assessment of 'single' control, by taking a substantive and functional approach and focusing on whether the purposes and the essential elements of the means are determined by more than one party. Joint control may

[55] *Cf.* Art. 29 Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor," adopted on 16 February 2010*, p. 32, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

take different forms and it does not need to be equally shared. Joint control does not involve 'joint and several' legal responsibility for the processing (56). However, a mere cooperation between various controllers does not entail any 'joint control'.

208 Thirdly, one of the main values of the EU data protection framework is the principle of data minimisation (cf. Art. 6). Observance of this principle is the responsibility of the controller. But in smart metering, the grid operators might be interested in collection of much more personal data than it is relevant, e.g. for increasing efficiency of the grid. They would also like to offer added value services on a commercial basis, often in co-operation with third parties (e.g. behavioural advertising).

209 Fourthly, the personal data can be retained only for as long as it is necessary to fulfil the purposes of their collection (Art. 6(1)(c)). Thus both the scope and length of the retention period matter for safeguarding privacy within smart metering. This issue is addressed in chapter 2.2 of this report.

210 Fifthly, the current framework empowers the data subject with certain rights concerning their personal data, e.g. the right to information about processing, to access them, to rectify any wrong or incomplete information, or to object their processing on a legitimate basis (Arts. 12 and 14). Due to the complexity of smart metering, it must be safeguarded that the data subject is well informed about processing, e.g. by a means of the consumer plaques on a meter. Furthermore, it must be clear what entity is the data controller (see supra) in order to allow the data subject to exercise their rights swiftly.

211 An example of providing transparency is ensuring adequate logging procedures to make sure subjects have insight into the data transferred outside of the meter. Included in the logging could be (among others) remote updates, changes to meter settings, meter commands and data transferred outside of the meter. Other use cases may exist.

212 Given the resources of a normal smart meter, it is not yet clear if it is possible to store all necessary data on the meter; if that is not an option, external storage is requires, which will require an access control system that is not entirely trivial. It is also important to use the data minimisation principle, and to ensure that only the subject can access this logging. The fact that physical access to the meter may be limited to the data subject and open to others (e.g. landlords, law enforcement) further complicates this.

213 Sixthly, the Data Protection Directive provides a number of legal bases for processing personal data. From the point of view of smart metering, the relevant ones are:

- unambiguous consent of the data subject (Art. 7(a));
- performance of a contract to which the data subject is a party (Art. 7(b));
- legal obligation to which data controller is subject (Art. 7(c));
- legitimate interest of the controller (Art. 7(f))[57].

214 For the sake of clarity, we must distinguish between processing personal data for the purposes of network operation (transmission and distribution), for supply of energy, and for added value services (i.e. any services other than those related to the supply of energy). The processing of personal data from or within a smart meter/ grid shall be done in accordance with Article 7 of Directive 95/46/EC, taking into account the Opinion 183 of Article 29 WP. Concerning value added services energy services, processing shall always be based on an unambiguous consent of a data subject, separately given for each value added service (i.e. 'opt-in' regime). The wording of such consent must be separately analysed.

---

[56] Opinion 1/2010, *op. cit.*, p. 33. See also: Jay R. (2010) *Important new guidance on the concept of "Controller" and "Processor" from The Article 29 Data Protection Working Party*, at http://www.apira.co.uk/documents/Pinsent%20Masons%20Concept%20of%20Controller.pdf.
[57] *Cf.* Knyrim R. & Trieb G. (2011) „Smart metering under EU Data Protection Law," *International Data Privacy Law, Advance Access*, at http://idpl.oxfordjournals.org/content/early/2011/03/01/idpl.ipr004.full.

215 Consent once given can be withdrawn, free of charge. This should be possible at any time, taking into account contractual law.

216 Seventhly, the Data Protection Directive requires the confidentiality (Art. 16) and security (Art. 17) of processing personal data. In addition, the controller must notify the supervisory authority before carrying out any processing operation (Art. 18). In many Member States, failure to notify is a criminal office (e.g. the Netherlands). In 2009 the ePrivacy Directive was amended to include the data breach notification (effective from May 11, 2011). Detailed regulatory provisions concerning data security within smart metering (Smart Grids) are needed, taking into account the characteristics of these instruments. In order to strengthen security, the concept of data breach notification shall be applied also to Smart Grids.

2.4.5. *Specific recommendations on smart metering and privacy protection*

217 The implementation of Smart Grids is perceived as a technological advancement that has many benefits. It could positively affect both consumers and market players. However, there are still many challenges associated. These risks are, among others, financial, privacy and security related.

218 So far, Smart Grids – at the EU level – are briefly covered by the internal electricity market framework as well as by the data protection legal framework. Smart Grids constitute a fairly new technology and these regulations evidently must be updated.

219 The following recommendations must be read together with the Commission's communication on the future of data protection in the EU[58]..

2.4.5.1. *General recommendations*

220 The following actions are recommended in general for smart metering:

a) to implement the Privacy by Design (PBD) principle, both at the legislative (i.e. legislation compliant with privacy and data protection laws) and at the technical level (i.e. through appropriate requirements in smart metering and Smart Grids standards to ensure that the infrastructure is fully consistent with these laws);

b) to implement the Privacy by Default principle, so that the most privacy friendly option is provided to the customer, as a default configuration, who can then adjust it to their own needs, thus possibly waiving some privacy;

c) to require the conduct of a privacy impact assessment (PIA) for each smart metering solution and environment and to make the results public. A wide range of interested parties (stakeholders) shall participate in such a PIA. Art. 29 WP should facilitate a template for member states to apply. It would be then to the member states to adopt and implement this PIA template.

d) Moreover, a general PIA might be drafted and sent for approval by the Art. 29 Working Party (as it was the case for the RFID);

e) It is recommended that the Commission enforce, and where necessary support member states on current privacy legislation implementation as research has shown that implementation is different from member state to member state

f) to require the opinion of the Art. 29 Working Party. It is recommended that the European Data Protection Supervisor (EDPS) works closely together with Art. 29 WP and the EDPS should give comments through Art. 29 WP.

[58] COM (2010) 609 final

2.4.5.2. Recommendations regarding protection of privacy

221 The following actions are recommended on the protection of privacy in smart metering:

a) Member states should ensure that appropriate privacy and data protection standards are implemented as a core part of their roll out of smart meters. This should include making sure customers have control over the collection and use of their consumption data.

b) in order to ensure a proportionate interference with the right to privacy:

i) regulators should ensure that each smart meter functionality complies with privacy and data protection framework

ii) to ensure that consent can be withdrawn at any time, taking into account any reasonable time basis and administrative burden for the controller.

iii) to clearly define the legitimate interval for measuring the consumption of electricity – member states should undertake use case analysis to ensure that appropriate level of consumption - information are collected.

2.4.5.3. Recommendations regarding protection of personal data

222 The following actions are recommended regarding the protection of personal data in smart metering:

a) regarding the allowed scope of data processed in smart metering:

i) to require the usage within smart metering of non identifiable personal data (anonymised or aggregated) to the highest possible extent;

ii) in case the personal data are to be collected and processed – to ensure due observance of the principle of data minimisation (Art. 6(b)-(c) of the 1995 Data Protection Directive);

b) regarding transparency of data processing:

i) to clearly distinguish the roles and responsibilities of each smart metering (grids) actor so that it is possible to determine who is data controller and data processor;

ii) to assess whether and how the concept of “joint control” applies to the data controllers within Smart Grids;

iii) to consider (meta)data logging procedures for storage and visualising of logging information in and status of the meters;

c) regarding legal bases for processing:

i) to clarify the application of the legal basis (bases) – e.g consent, legitimate interests, compliance with legal obligation - for the processing of personal data within smart metering (grids);

ii) to irrevocably require a separate, prior, explicit and informed consent of a customer (consumer) for the processing of their personal data within smart metering for each added value service;

d) regarding data security:

i) to include the data breach notification in the said framework;

e) regarding consumer empowerment:

i) to establish a consumer privacy notice is available to customers in a clear intelligible form that also specifies their rights in relation to the data;

ii) ensure that consumers can easily exercise their rights (especially data subject rights as provided for in Directive 95/46) in smart metering/grids;

iii) to require awareness-raising measures for the consumers (training, information, etc.) as a complementary tool.

EG2.P.11 It is recommended that specific measures are taken to ensure the adequate protection of personal data in smart metering. The fact that smart metering may be necessary for the society as a whole should not suffice to override the fundamental right to protection of privacy. Any solution must comply with the law on data protection and privacy. This position has also been supported by the opinion of Article 29 Data Protection Working Party.

3. Security in Smart Grids

3.1. Smart Grid Information Security (SGIS)

223 Cyber threats, intentional and unintentional are a fact and growing. These threats range from Distributed Denial of Service (DDoS)-attacks, spreading malware and leakage of data to indeliberate ones like software errors, technical failures but also outages through natural disasters. During the development of the Smart Grid, cyber security needs to be addressed. The general awareness about cyber security shall increase over the coming years, also for our critical electricity infrastructure. It is impossible to mitigate all cyber related threats while maintaining a Smart Grid, but the owner must be prepared and take due care. Therefore the level of 'smartness' should always be considered in relation to the cyber-related risk, cost, public image and consumer trust. Risk mitigation measures shall be one of the main goals in securing the Smart Grid. A Smart Grid needs to be hardened to prevent unauthorised entries or other uncontrolled activities that threaten the confidentiality, integrity or availability of the Smart Grid. The protocols used must be able to transfer information secure. Detection systems and firewalls must guard critical parts of the infrastructure. Countermeasures must be in place to be able to handle against cyber security incidents, to minimise eventual damage. The role of security[59] is to address these concerns and to create a sustainable secure environment for Smart Grids.

224 Improvements in information security increase the robustness and resilience of a Smart Grid from both a physical and a cyber perspective, thereby reducing the probability and consequences of e.g., manmade mistakes, technical failure, deliberate attacks, and natural disasters. Also resulting in improved restoration times following storms and other natural events, reduction in injuries and deaths of employees due to the reduction in time spent in hazardous situations and the availability of more intelligent systems that support worker safety conditions and the reduction in the probability that a deliberate man-made cyber-attack could occur and a reduction of the consequences of any attacks that are not detected or prevented. These benefits will decrease the probability that extended outages impacting the security of customers will occur by reducing the threat, vulnerability, and consequences of disruption.

225 The increased reliance on Smart Grid technologies will require the deployment of new systems to address cyber security ensuring that the functioning of this critical infrastructure is robust and resilient. Part of that is that the Smart Grid needs to be as 'hack proof' as possible (27), but also that the design takes into account a wide variety of threats even including space weather effects. Critical infrastructure (components) should be separated from not critical infrastructure through levels of physical, technical (ICT) and organisational security controls.

226 Increasingly, more computer controls are installed to manage the power market operations (buying and selling), generation, transmission, and distribution. Supervisory Control and Data Acquisition (SCADA) systems are managing power flows and grid security by controlling substations, transformers and generators. Those SCADA systems get and send signals out to sometimes thousands of devices on the grid to balance the electric load and demand as well as the power flows through the grid. The signals are most often sent via internal computer networks and sometimes by radio. Unfortunately, many of the devices also have other connections, multiple connections, sometimes also direct connections to the public internet, for instance to permit manufacturer's remote diagnostics. What that means is that if you can hack from the internet into the control network, you can give commands to devices on the grid. Therefore, it is an absolute must to minimise the accessibility of critical infrastructure (components) and Smart Grid network facilities from the internet and other networks. (Remote) access solutions to the Smart Grid by third parties for maintenance and or troubleshooting should always be deployed in a manner to mitigate cyber risk. DHS (Department of Homeland Security) in the US and CPNI (Centre for Protection of National Infrastructures) in the UK provide a report on configuring and managing remote access to for Industrial Control Systems[60]. This report is also applicable to the Smart Grid.

227 Thus the industry faces three challenges: (i) provide architectures and devices that offer a high grade of automation to run such Smart Grid as a responsibility of multiple organisations, (ii) develop Smart Grid

[59] A code of conducts could also play an important role in security, by establishing a culture of collectively address security and live up to agreed upon system requirements.
[60] Configuring and Managing Remote Access for Industrial Control Systems, CSSP DHS and CPNI, November 2010.

solutions that follow security by design from the beginning, and (iii) to develop efficient Smart Grid components and networks that offers a future proof and sustainable solution regarding functionality and security.

228 The U.S. National Institute of Standards and Technology (NIST) published in September 2010 guidelines for Smart Grid Cyber Security in NISTIR 7628 (28) in which many of these issues have been addressed.

3.1.1.Information Coordination

229 While the Smart Grid is a complex, widely distributed ecosystem with numerous different players, there seems to be insufficient coordination for a proper estimate on what issues have been addressed by whom, and which party has to establish what kind of responsibility and authority.

230 For example, while individual organisations have performed penetration tests on actual Smart Meters, the results have been largely held confidential. Thus, it is difficult to judge whether the general implementation status of smart meters is sufficient in terms of security, or if critical functionality should be moved towards organisations with more experience in designing secure hardware, e.g., by recommending use of smartcard-like co-processors. There are experiences with Smart Meter roll-outs in a number of Member States (e.g. Italy and Sweden). Up until now, there have not yet been signs of significant security incidents.

231 More coordination is also required to assure transparency in decision making processes – projects of the financial scale of the Smart Grid implementation do tend to need special scrutiny to assure the technologically most appropriate solution embedded in a right organisational and legal context.

3.1.2. Roadmap

232 The first 'gap' in this is that there seems to be an insufficiently worked out roadmap. Such a roadmap has to provide clear objectives on what a Smart Grid – in European context – initially should have as objectives and functions. Thereafter, a plausible division on how to incrementally introduce parts of the Smart Grid, and a division on which entities should have what responsibilities without taking into account best practices and experience– examples here are secure implementation of the embedded systems (meters, substations, etc), or the handling of the vast amounts of data that the Smart Grid may generate. This is discussed further in the report by Smart Grids Expert Group 1 and 3 (29) (17).

233 In the Smart Grid setting, a solid European-wide roadmap is especially challenging as the overall system requires expertise in multiple domains and – to some extent – the long term vision is such a large step ahead that the concrete future use cases with a good economic underpinning are unclear. This makes it especially important to have a Smart Grid roadmap that aims for a modular design geared towards evolutionary growth. That approach will also give the industry the certainty that components implemented now will not be obsolete in a few years when standards evolve.

3.1.3. System Architecture

234 System Architecture should support the overall vision in terms of business objectives. Given the complexity of the Smart Grid network, the main technical gap is the lack of an overarching architecture that reflects the different components, their roles and their criticalities, and from which lower level architectures for the subcomponents can be derived. The architecture has to define a strong logical separation of components and functionalities, and define access controls and communication restrictions to assure system integrity (for example, using a variant of the BIBA model.

235 An important aspect in the architecture we envision is that it shall allow for an evolutionary growth, and support future developments that at the current time cannot be foreseen. This requires an open architecture with a definition of clean interfaces, and a way to add new components without endangering the integrity and availability of the existing ones. Special attention needs to be devoted to interfaces with third party services and home area networks, which will expose the network to very open and-or extremely resource restricted (and thus less trustable) components.

236 Currently, there is no publically available reference architecture for Smart Grids with references to how privacy is designed into the core functionality, referring to all standards and principles for IT systems, business practices, and physical designs and networked infrastructures.

237 The - to be developed - reference architecture should be derived from Smart Grid operational and business models, amongst others from the ETSO harmonised electricity market role model, and include the Smart Grid information security model (Smart GridIS) and data protection / privacy model (DPP). Essential requirements needs to ensure that the Smart Grid information system provides state-of-the-art protective measures in line with legal compliance with data protection / privacy directives, measuring instruments directive, duly e-business operations and more.

238 The Smart Grid information security essential requirements need to be ensured – for both:

- essential requirements and primary protection goals common with the ICT sector;
- essential requirements specific to the energy sector.

239 Those sector specific essential requirements are different from the common requirements. In the electricity grid there also needs to be differentiation between requirements for critical infrastructures and those for infrastructures supporting Smart Grid energy services. There are also several classes of data handled in Smart Grids that need appropriate security levels. For several Smart Grid data protection classes (Smart Grid-DPC) legal requirement exist.

240 Top down 'system level' requirements need to be included in the standards for all stakeholders participating in the Smart Grid – i.e. standards for products / solutions / services and the standards for organisations in their specific market roles.

241 The Smart Grid operational and business models will keep evolving for a long time to comply with the continuous evolution of functionality, with ever changing impacts on the Smart Grid information systems supporting the availability of sufficient energy supply and the availability of today's and future energy services. Due to that the information system and the requirements for information security and data protection / privacy will keep evolving.

3.1.4. Device & Implementation Security

242 Experience with already existing meters or their components shows that implementation of security in a number of cases is so far neglected, and that there is a realistic probability that deployed meters will contain security vulnerabilities. This may partially be due to lack of experience in secure implementations. Many developers for embedded systems have never been required to write secure code, focusing on safety.

243 Moreover, cost and resource constraints (if hardware resources are reduced to the minimum necessary for operation, security provisions are likely to be sacrificed for memory) and performance reasons can negatively influence security. The last roadblock towards a secure implementation is that so far, this has been considered a vendor specific issue. While protocols and architectures are likely to follow industry standards and thus will involve professional security analysis and reviews, individual smart meter implementations to our knowledge so far are just deployed as is.

3.1.5. Assurance

244 Given that security is difficult to measure and define, an assurance strategy is required both on component- and on system level. This strategy needs to cover business continuity as well. This also will give more ability for manufacturers to plan, as they know what components they can buy safely, and if their own products satisfy the necessary standards. A good assurance strategy will also assure that manufacturers that invest into appropriate security are not punished by the market by having higher prices due to a non-functional component.

3.2. Cyber security

245 As already mentioned, cyber security incidents happen, due to operational, technical or design failure, human error as well as man-made attacks. Miscreants continue to infiltrate networks and exfiltrate sensitive and

proprietary data upon which the world's economies depend every day. A good example is the coordinated covert and targeted cyber attacks that have been conducted against global oil, energy, and petrochemical companies. These attacks, named Night Dragon, have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. Another example of a targeted attack that hit the headlines recently was Stuxnet, a sophisticated computer worm that was aimed at a uranium ultra-centrifuge plant in Iran where it caused serious damages.

246 Electricity companies also have been hit by (cyber) incidents in recent years and showed that the power grid and other energy infrastructures are vulnerable to both cyber disruptions (due, e.g., to malware) and from outside attacks using cyber methods. A compelling example of how different types of incidents (cyber and non-cyber) often come together in an major incident have been seen in the extensive blackouts in the North-eastern US and Western Europe during the late summer and early fall of 2003. They demonstrated in a convincing way the fragility of the energy infrastructure and the possibility of cascading power grid failures due to a combination of problems amongst which problems with control system hardware and/or software.[61]

247 An article by Averill and Luiijf[62] states that 'for obvious reasons, to date no government, utility, or energy company has officially stated that a major power outage or similar event has been caused by a cyber attack. That being said, numerous reports have appeared attributing specific incidents to cyber attacks. Although reports from the CIA do not name specific countries, they do claim that in at least one case, multiple cities were affected, and that the attacks were subsequently followed by blackmail or extortion attempts. Perhaps the closest thing to a smoking gun is a series of power outages in Brazil in 2005, 2007, and 2009. Brazil has steadfastly denied that a cyber attack occurred in either 2007 or 2009, attributing the 2007 outage to 'sooty insulators' on high-voltage lines. In contrast, a number of analysts believe that at least the 2005 event was due to Supervisory Control and Data Acquisition (SCADA) disruptions caused by hostile intrusion via the internet.

248 Moreover, malware and hackers are known to have penetrated numerous times into critical supervision parts of the power grids in Australia, Europe, and the U.S. Examples include nuclear power plants being shut down due to cyber disruptions, near loss of control of a national control system in Australia due to malware, and a hacker who was able to wander around in a large European transmission system operator's grid for 10 days.'

249 The same article by Averill and Luiijf states that 'classified reports from around the globe indicate that main SCADA operator consoles of both refineries and large chemical plants have been penetrated by hackers for days. Similarly, malware has penetrated control systems on offshore oil and gas platforms a number of times, resulting in the risk of uncontrolled release of gas or oil and potential environmental damage, as well as possible explosions and loss of the platforms.

250 The article continues stating that ' "Red Teams" of mock intruders from the US Department of Energy's four national laboratories have devised what one government document listed as 'eight scenarios for a SCADA attack on an electrical power grid' -- and all of them worked. At least eighteen such exercises have been conducted against large regional utilities over the last several years. In 2002, Richard A. Clarke, President G. W. Bush's cyber security adviser, was quoted as saying that 'the intruders ... have always, always succeeded.' Subsequently, many more red team intrusions have been attempted, and all but one were successful. In the one unsuccessful attempt, the Red Team was forced to break off its penetration because hackers from a foreign nation were simultaneously penetrating along the same path'.

3.2.1. Key Vulnerabilities

251 But what does this mean for the security of Smart Grids? The Smart Grid vision and its increased reliance on ICT systems and networks expose the electrical power grid to potential and known cyber security vulnerabilities

[61] Technical analysis of the August 14, 2003, Black-out: What happened, Why and What did we learn?, Report to the NERC Board of Trustees by the NERC Steering Group, July 13 2004

[62] B. Averill and H.A.M. Luiijf, Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention, Int. J. on Energy Security, 18 May 2010

associated with using such systems, which in turn increase the risk to the smooth and reliable operation of the electrical power grid. These potential vulnerabilities[63] of Smart Grids include:

- increasing the use of ICT-based systems and networks increases the number of entry points and paths that can be exploited by potential adversaries and other unauthorised users;
- increasing the use of new system and network technologies can introduce new, unknown vulnerabilities to the power grid;
- interconnecting ICT-based systems and networks (that can be wirelessly and/or remotely administered) can allow adversaries wider access and the ability to spread malicious activity. Especially wireless or radiofrequency telecommunications could make the Smart Grid susceptible to eavesdropping, jamming or manipulation;;
- increasing the amount of customer information being collected by IT-systems (and transmitting it via networks) provides monetary incentive for adversaries to attack these systems, and could lead to the unauthorised disclosure and use of private and privacy-sensitive information;
- the reliability of most of the current ICT-systems and network components and their architectures is far less reliable and fail-safe than power grid components and therefore may introduce a less reliable power supply to the customers. E.g., just a cable cut by a steel beam near a major Smart Grid data processing node may negatively affect situational awareness and abilities to control. The loss of power to such a node may even show effects of mutual dependencies of power and ICT.

252 A big concern in the electrical power industry is the vulnerability of industrial control systems; particularly the SCADA systems that are used to control dispersed physical assets or devices from a central location. These SCADA systems were originally hard-wired systems primarily that were used to control processes at a single site. They were never designed to be connected to the outside world and believed to operate in a benign environment. However the world has changed. Cheap PCs, improved telecommunications and the internet, have connected these individual power grid sites to one another and, in many cases, to the outside world via the internet, often through the office networks. This increase in connectivity is pushed by the liberalisation of the energy market. Business needs more and more production data for management purposes. An example of this is that het energy production companies need to continuously share their production and reserve capacity data with market operators and transmission system operators directly or indirectly from their SCADA-controlled systems.

253 The increase in connectivity also introduces vulnerabilities. The control systems are intrinsically vulnerable to any intruder who can penetrate a company's firewall (or to unintentional intrusions caused by unsafe browser settings or employee actions, such as neglecting to scan an attachment for viruses before opening) or plugging in a malware infected USB stick in the control system. Another concern is the unwanted (remote) access by intruders, sometimes being insiders or third-party engineers. The use of wireless access points which are sometimes used in production environments, doesn't help in this aspect, since it can be exploited by attackers.

254 Most non-specific forms of malware will essentially shut down an operating system. Industrial control systems are even more sensitive to malware than for example a regular laptop. Of much more concern, however, is systematic exploitation of vulnerabilities by criminal or even terrorist organisations for financial or political gain. In particular, the high value of the commodities flowing through the grids or networks makes them very attractive targets for exploitation by criminal elements, either by means of fraudulent transfer of funds, rerouting of energy flows, or by extortion attempts.

255 An example of this was given in a rare public warning to the power and utility industry, when a CIA analyst said that cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities[64]. The CIA analyst was

[63] GAO, Electricity Grid Modernization: Progress being made on cyber security guidelines, but key challenges remain to be addressed, report GAO-2011-117, January 2011.
[64] *Hackers Have Attacked Foreign Utilities, CIA Analyst Says*, E. Nakashima and S. Mufson, Washington Post, January 19, 2008; Page A04

speaking at a trade Conference in New Orleans attended by representatives of US and international security officials from the government and from power, oil and gas companies. The speaker reported that the CIA suspects the attackers to have profited on inside knowledge.

256 Next to this intentional threat, also unintentional actions can cause a lot of damage and therefore be a threat. A good example of this was the emergency shutdown of a nuclear power plant in Georgia after a software update was installed. The incident occurred on March 7, 2008 on the Hatch nuclear power plant near Baxley, Georgia65. The trouble started after a software update was installed on a computer connected to the plant's business network. The computer was used to monitor chemical and diagnostic data from one of the plant control systems, and the software update was to synchronise data on both systems. When the updated computer rebooted, it reset data on the control system, causing safety systems to interpret the lack of data as a drop in water reservoirs of the plant cooling system.

257 Business continuity is one of the most crucial aspects in electrical power companies, but despite this top management of these companies still do not fully recognize the risk of cyber disruption to their operational processes. This is slightly changing with the introduction of the Smart Grid. Companies start to realize that with further introduction of the Smart Grid the telecommunications infrastructure is getting almost as important as the traditional electrical grid and even point out the telecommunications infrastructure as the Third Grid (next to electricity and gas grid). The following step is that management also realise that the increasing connectivity enhances the vulnerability of the control systems, because they become more and more connected and more attack vectors are provided. Unfortunately, energy and other sectors lack a professional, worldwide incident-reporting mechanism. Energy systems are so critical to our societies that an approach similar to the incident-reporting system used by the international air transportation industry is urgently needed.

EG2.S.1 An important task for the European Commission is the creation of a trusted network of public and private organisations, where information about incidents, threats, vulnerabilities and good practices will be shared intensively. Point of departure is that companies themselves will only take effective measures if they have access to the right information and are able to make accurate risk assessments. The participants can prevent incidents themselves. This will safeguard the European economy as a whole and the continuity of the individual organisations at the same time. ENISA can play an important role in facilitating this Information Exchange within the electricity sector, but also with governments, IT & Telecom providers, vendors & integrators, academia and research institutions. Existing information exchanges like the EuroSCSIE (European SCADA and Control Systems Information Exchange) can form a good basis for this.

3.2.2. The opponents

258 Cyber attacks are carried out by a variety of actors with different motivations, but it is convenient to consider four different categories[66]. Averill and Luiijf give an overview of possible opponents, where they state that 'In order of increasing capability and threat, they are recreational, activist, criminal, and state-sponsored. Recreational hackers are largely motivated by the challenge of demonstrating their ability to hack into a protected server. The nature of the server (industrial vs. commercial vs. governmental) is often of secondary importance. Recreational hackers are often young and technically opportunistic, trolling many servers to locate one that they are able to penetrate. Because due care on the part of the system operator will keep them out (at least most of the time), they constitute by far the least serious threat to energy infrastructure.

259 In contrast, the other three types of hackers tend to target specific servers in order to advance a specific agenda. Activists (often referred to as 'hacktivists') view cyber attacks as a tool that allows them to advance a particular political, social, or economic issue.

260 Criminals view cyber attacks as a tool that allows them to make money easily with minimal risk of apprehension. They tend to not be highly specific with regard to targets, but are highly opportunistic in exploiting perceived vulnerabilities that can generate revenue. In the energy sector, this could lead to

---

65 *Cyber Incident Blamed for Nuclear Power Plant Shutdown*, Brian Krebs, Washington Post, Thursday, June 5, 2008.

66 B. Averill and H.A.M. Luiijf, *Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention*, Int. J. on Energy Security, 18 May 2010

manipulation of specific markets or to extortion by threatening to disrupt the electrical power grid unless a fee for 'protection' is paid.

261 Finally, state actors have a variety of possible motivations, including commercial, military, tactical, and strategic. In many countries, the distinction between the public and private sector is not as well defined as in others, and cyber attacks can be used to install portals for automatic export of sensitive commercial data to further the business objectives of a nationally owned company. The potential use of such techniques to obtain sensitive military or government information to advance national interests is obvious. More importantly, however, state actors can also leave behind hidden re-entry gates that could be used as a tactical or strategic attack point in an international confrontation. Disrupting energy flows within a country could certainly create chaos, forcing the target nation to divert attention and manpower to dealing with internal issues rather than an external conflict.'

262 Though hackers from various countries outside of the EU have attracted the most attention in the headlines that address cyber security issues, the most potentially damaging attacker, however, is a technically competent insider, more often than not a disgruntled employee or a person acting for political or ideological reasons. They bypass normal security procedures mandate extensive screening of personnel with administrator-level access to control systems. One example of an insider attack is provided by the actions of an information communications technology (ICT) contractor for an oil and gas field developer, who, upon learning that he would not be offered a full-time position, reprogrammed the company's control system to disable its leak detection ability.

263 However, as already mentioned before, the biggest cyber security risk is not in these opponents that intentional try to sabotage the systems. Unintentional threats, mainly by lack of awareness by company or third party employees pose a far bigger threat. A lot of incidents occur because employees of hired personnel hook-up their sometimes contaminated laptops to the control systems or by the use of USB thumb drives of questionable origin (not realizing that they could have been pre-loaded with malware), bypass security controls in order to connect secure process control networks to the outside world, and allow third party engineers to connect contaminated laptops to the network.

3.2.3. Future Challenges

264 Knowing all this and realizing that the next big cyber security concern looming on the horizon is provided by the impending widespread implementation of Smart Grid technology, which is a critical component of 21st century energy systems, some challenges can be identified.

265 Several expert bodies around the world tried to identify these challenges to securing Smart Grid systems. The U.S. Governmental Accountability Office[67] identified the following six key challenges:

- Aspects of the regulatory environment may make it difficult to ensure Smart Grid systems cyber security.
- Consumers are not adequately informed about the benefits, costs, and risks associated with Smart Grid systems.
- Utilities are focusing on regulatory compliance instead of comprehensive security.
- There is a lack of security features being built into certain Smart Grid systems.
- The electricity industry does not have an effective mechanism for sharing information on cyber security.
- The electricity industry does not have metrics for evaluating cyber security.

266 Within Europe the Ad Hoc Expert Group on ICT security and resilience of the Smart Grid that was convened by the European Commission (EC) with the support of the European Network and Information Security Agency

[67] GAO, Electricity Grid Modernization: Progress being made on cyber security guidelines, but key challenges remain to be addressed, January 2011.

(ENISA)[68], expressed their points of view about the ICT security and resilience challenges for the Smart Grids. In particular, they raised concerns about the availability of ICT systems and the impact it could have on Smart Grid, the need for additional security issues when specific SCADA systems are made accessible via the internet, and the role of governmental authorities. The Expert Group raised the following key points:

- Interdependencies between ICTs and Energy should be identified. Furthermore, there should be guidelines in place and recommendations for the improvement of the SCADA systems, security issues should be included in SLAs, and the smart metering system must be improved and recommendations must be proposed for further actions.

- Information sharing on security breaches and architecture is essential and presents a basic condition to protect Smart Grids. Information sharing within and between sectors and the government is important. Determining how to safely communicate vulnerabilities and attack vectors is key to vendors and end users.

- ICT and energy security experts should work together to enhance the design of security in Smart Grids.

- Among the policy drivers to secure the supply of energy there is a need to increase the grid robustness and resilience, as well as the integration of large centralized and small distributed generation. Although ICT security and resilience of the Smart Grids are not now specifically considered among the current policy drivers, an approach should be designed to bring together the ICT sector and the Energy sector.

- There is a need to fix a common definition for Smart Grids, as well as a reference model and a clear identification of threats. A reference model is needed for smart home appliances, for distribution system operators, for the end-user renewable energy production to grid, smart metering, distribution grid, transmission grid, market operators, and for power exchanges.

- To counter the factors that threat some areas such as the privacy of citizens or the manipulation of smart meters there is a need for better hardware and software reliability.

- Energy supply core functionality requirements should include: uninterrupted service, black start capability and little dependencies on other critical infrastructures. Also, all functionalities need to be robust and resilient. Furthermore, the less critical processes on energy supply should not endanger the more critical ones. Processes should be able to handle disruptions and return to normal operations afterwards. These requirements should be fulfilled even in case of breakdown, failure or targeted attacks to the ICT architecture of the Smart Grids. The impact of ICT problems on energy delivery should be kept as low as possible.

- The Smart Grid increases the sophistication of automation and communications in areas such as smart islanding and increased demand side management, which also introduce additional interfaces and players involved. This automation will involve increased monitoring, measurement and control which are reliant upon ICT.

- The Smart Grid brings with it a new set of technologies and threats. Policy makers need to work with regulatory bodies to establish standards, security guidelines and compliance mechanisms. This approach will provide consistent guidance, a level playing field and incentives for compliance.

- The security of the grid will rely heavily on the use of public key cryptography. Therefore, the EU needs to consider which standards of public key cryptography should be used. Closely associated with this is the corresponding public key infrastructure (PKI), including certification authorities. Policies for certification authorities need to be developed to address the cross border nature of the grid.

[68] The ad hoc Expert Group on ICT Security and Resillience of the Smart Grid (1st conference 18 November 2010). The first meeting of the Ad Hoc Expert Group on ICT security and resilience of the Smart Grid was convened by the European Commission (EC) with the support of the European Network and Information Security Agency (ENISA), within the framework of the policy initiative and Action Plan on Critical Information Infrastructure Protection (CIIP)1 adopted on 30 March 2009.

267 These points are not part of the set of recommendations as provided by Expert Group 2 in this report, but are considered to be relevant in the security of Smart Grids.

EG2.S.2 Energy supply core functionality requirements should include: uninterrupted service (subject to allowable disconnection and prepayment usage), black start capability and little dependencies on other critical infrastructures. Also, all functionalities need to be robust and resilient. Furthermore, the less critical processes on energy supply should not endanger the more critical ones. Processes should be able to handle disruptions and return to normal operations afterwards. These requirements should be fulfilled even in case of breakdown, failure or targeted attacks to the ICT architecture of the Smart Grids. The impact of ICT problems on energy delivery should be kept as low as possible. Regarding smart metering this would mean that failures within parts of the smart metering infrastructure including the used ICT-networks must not lead to blackouts or impair other processes more critical for electricity delivery more than unavoidable. It is recommended to follow a threat and risk-based approach towards privacy and security of Smart Grids in alignment with EU guidelines and policies. ESOs to ensure principles are reflected in standards.

3.2.4. The Road Ahead

268 What are the key points to focus on? Everybody seems to realize that securing the smart gird isn't something that any organisation could do on its own. A concerted and cooperative effort by academia, manufacturers, industry leaders, and policymakers is required to secure the Smart Grids against disturbances and misuse. Top priorities are:

- (top) management awareness at the electricity companies;
- information exchange;
- security by design;
- guidelines, requirements and certification;
- the human factor.

3.2.5. Top management awareness

269 Perhaps the most crucial requirement is top management awareness at the electrical power companies, since these companies have to implement the measures to increase the robustness and resilience of the Smart Grid. Top management needs to be aware of the risk and take appropriate action, e.g. by including cyber issues in policy and in business continuity plans.

270 To raise this awareness it will be important to investigate and act upon incidents in a cooperative international fashion, rather than being neglected or downplayed. Parallels can be found in the way that the aviation industry handles near misses and crashes. In the Netherlands a brochure 'Process control security in the Cybercrime Information Exchange' was written especially targeting this management layer. These kind of good practices must be exchanged between countries. ENISA can play an important role in the stock taking and exchange of these good practices.

3.2.6. Information Exchange

271 Because companies take measures based on a risk based approach, it is very important to provide these companies with timely information about incidents, threats, vulnerabilities and good practices. A requisite for successful (public-private) information exchange is bringing people together in strong, permanent networks, where trust is build and value is added, sectoral and cross sectoral, national and international. In some countries like UK and The Netherlands[69] trusted public private information sharing initiatives are in place and provide extra value to all participants, within sectors but also cross sectors. Also international information exchanges exist, like the European SCADA and Control Systems Information Exchange (EuroSCSIE) and the MPCSIE (Meridian Process Control Systems Information Exchange), information exchanges where the security

69 Information Exchanges of CPNI in the UK and the Cybercrime Information Exchange of CPNI.NL in The Netherlands.

of Smart Grids is an important topic. This exchange of information raises the security bar. The European Commission can play an important role in facilitating these information exchanges on the European level. ENISA already started to participate in the EuroSCSIE and should continue to do this. National Information Exchanges are needed to further spread the information within the countries themselves. Also here recent work of ENISA should be a priority in the upcoming years.

272 This information exchange should take place on different levels, strategic, tactical as well on the operational level. The European Commission can play a strong role in bringing together CIOs (and possibly CEOs) from energy companies, government agencies, and network security providers to discuss details about actual incidents behind closed doors. The key is to convince participants that revealing weaknesses that they have overcome is an effective way to learn about potential threats before they happen, so that companies can take appropriate actions based on the risk involved. National governments need to drive the creation of a cross-sector national plan to improve cyber security in the Smart Grids. These governments should facilitate the public-private exchange of information and also could prove to be a crucial source of threat information, good practices, and technical support for various industry players.

EG2.S.3 The European Commission should play an important role in creating awareness of the importance of security while implementing Smart Grids. This should be done on all levels, but the EC can play especially have an important influence at the CEO-level in the electricity industry, but also cross-sectoral in the telecommunications industry. It would be a good idea introducing this strategic level at a Ministerial top conference on the security and privacy of Smart Grids, with the aim of producing a joint public-private roadmap to secure Smart Grids.

3.2.7. Security by design

273 The best way to prevent incidents is to deploy technologies, systems and networks that are designed, built, and tested to achieve secure operation. For this we rely on the ingenuity of the R&D community and the manufacturers of hardware and software used to build the Smart Grids, but also on the telecommunication sector providing resilient infrastructures. It also takes operators that ask for (and also wanting to pay the price) of these secure solutions. The utilities will have to participate by specifying security-by-design when procuring new systems or solutions. Owners and operators will also work with vendors to collaborate on improvements to built-in security. Important is to include end-to-end security solutions and to find suitable solutions for the legacy systems that are part of the Smart Grid eco systems.

274 What can be already stated by today is that electronic certificates will play an essential role in security concepts. The EU needs to consider which type of public key cryptography it will standardise on and what the minimum lifetime of the solution shall be. Closely associated with this is the corresponding public key infrastructure (PKI) including certification authorities. Policies for certification authorities need to be developed to address the cross border and multiple organisational responsibilities nature of the grid. Costs being related to security may not become a show stopper for Smart Grids. The availability of publicly available trust centre functions when they are instated is preferably free of charge. DSOs and metering infrastructure operators that run Smart Grid devices like smart meters need such kind of generic security services prior to the start of new device rollouts.

275 In this design also physical security should be taken into account. People and computers find themselves in a physical environment. This is susceptible to calamities and increasingly the target of threats. Fire can reduce a data centre to ashes. So we must think carefully about back-up systems and their physical location. The power supply can be sabotaged. Old-fashioned burglary goes hand in hand with cyber threats.

EG2.S.4 A trusted smart meter infrastructure will eventually very likely be based on certificates being released by certification authorities. It is recommended that national certification authorities are involved in Smart Grids prior to a roll-out of devices. These national authorities (similar to or even included in Data Protection Authorities) can operate a national trust centre. It is recommended to make sure the implementation of these certification authorities and trust centres is done at the Member State level, although alignment within the EU is important to prevent difficulties for internationally operating actors and guarantee a level playing field. High investments needed for certification of devices may hinder their introduction.

3.2.8. Guidelines, requirements and certification

276 Additional guidelines, requirements and certification of products and practices can provide a baseline for secure Smart Grids and cover a lot of the challenges provided. The last year several interesting public private initiatives in this arena to raise the security bar where published, like NISTR 7628 'Guidelines for Smart Grid Cyber Security'[70], the BSI initiative for common criteria protection profiles for gateways and security modules[71], the WIB 'Process Control Domain Security Requirements for Vendors'[72] including a certification protocol for vendors and the framework document 'Privacy and Security of the Advanced Metering Infrastructure' of the Privacy & Security Working Group of Netbeheer Nederland[73] in the Netherlands. On a European level these guidelines, requirements and certification protocols should be consolidated.

277 The implementation of Smart Grid does require a major process change for today's utilities maintaining the power grid, especially for the security processes. Many components and processes in the Smart Grid must be treated secure. Maintenance and ICT staff must be aware of the security guidelines but also of the issues and risk. Security assessment will become a standard program within the processes of the Smart Grid owners and all industry players. Smart meters should not be rolled out until end-to-end testing and certification of the smart metering system has been conducted.

3.2.9. Human Factor

278 Cyber security does not restrict itself to hardware and software. The human factor is crucial, because people make mistakes as was pointed out in some of the examples given before. People act carelessly when it comes to passwords and security regulations, like the usage of USB-sticks or other portable media. Therefore a change in behaviour is needed. People must be aware of the risk; understand what the impact of acting incorrectly is and ensure they follow regulations and procedures. Training and exercises are essential to realize this goal. Some companies already started to provide continuous cyber security training and education to their employees, sometimes face-to-face, sometimes through web based modules. Good practices should be shared within the information exchanges mentioned before.

EG2.S.5 Within a trusted network of public and private organisations the European Commission can promote and facilitate: the **development** of security guidelines for Smart Grids, keeping existing guidelines like the NISTIR-7628 in mind; the **certification** of products and services (similar like the Certification Program that was built for the Process Control Domain Security Requirements for Vendors from the WIB); **test facilities**, where new architectures and it's components can be tested; **Research & Development** in the area of the security and privacy of Smart Grids. A periodic **check** on adequacy of measures taken (such as the International Security Forum's health check) can aid in the awareness of the current effectiveness.

EG2.S.6 The level of experience and awareness can be increased within a trusted network of public and private organisations by providing (online) training and information facilities.

[70] NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements by the The Smart Grid Interoperability Panel – Cyber Security Working Group, August 2010

[71] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile

[72] WIB, The International Instrument Users' Association. WIB provides process instrumentation evaluation- and assessment services for- and on behalf of- its industrial user member companies. WIB operates in close collaboration -through the 'SWE' federation- with 'sister' Associations, EXERA in France and SIREP/EI in the UK. A co-operation agreement exists with the NAMUR organisation in Germany.

[73] Netbeheer Nederland' is the association representing the interests of electricity and gas network operators in the Netherlands.

4. Measuring

4.1. Measuring Instruments Directive

279 Smart Metering components need to comply to the measuring instruments directive. The components are critical system components within Smart Grids. Smart meters and the logical and physical system components contain and process personal data at the highest level of detail. The Measuring Instruments Directive 2004/22/EC (19) provides requirements for smart meters and other measurement components.

280 The Directive describes for several classes of measuring instruments what the technical requirements are. Among these instruments are smart meters. In order to show conformity to MID requirements and to be acceptable for use meters should be tested and marked with the CE conformity mark. The Directive currently does not involve privacy-related subjects and does not focus on other devices within the Smart Grid infrastructure.

4.1.1.Smart Grid Meter System

281 The Smart Grid Meter System components are logical blocks covering the Metrological domain and the Energy Management Domains. Its logical building blocks may be integrated in different physical products or reside inside one enclosure. In any case the interfaces between the logical building blocks exist and should fulfil state of the art information security levels. Each of the logical building blocks consist of a substructure – i.e. within the logical building block 'meter' there are metrological sensors and actors and an integrated display (required by the Measurement Instrument Directive).

282 Smart Grids contain many more logical 'building blocks' that may benefit from regulation as they have an influence on measuring data, e.g. (depending on implementation) Energy Management Gateways, Energy Managers and Meter Gateways. These functionalities may be incorporated in different types of physical devices (e.g. Energy Management Gateways in DSL routers). This may complicate MID regulations as a wide variety of components needs to be assessed. Focus should lie on the functionality of a device and not on the product itself. In order to adequately protect personal data and other data protection classes (SG-DPC) within the Smart Grid information system there is also a need to assess these functionalities in conjunction with their interfaces (i.e. the communication between the devices).

283 According to Privacy by Design and Privacy by Default – there must be precautions inside the Smart Grid Meters System to handle the different SG-DPC in all cases – when data is captured, processed, transmitted/received, stored and erased in the various logical building blocks of the Smart Grid meter – and the Energy Management System including its sub components. The access to the SG-DPCs needs to be based on roles and identities, i.e. when transmitting to the Market Roles as defined by EG3 report (17) or when transmitted inside the building – and even when transmitted to the display included in the Smart Grid meter system (as required by the MID).

284 Also there is a need to manage the access rights for all actors (individuals- their IDs, roles, groups or technical actors and their credentials), defining rights and obligations within the Smart Grid Meter System and the Energy Management System.

285 The measuring instruments directive requires displays to enable consumers to validate their bills.

286 The measuring instrument directive needs to ensure that the data collected from the sensor is stored in the meter only with a qualified signature (that must be unchanged End-2-End) – ready for transition and display – so meter data includes the originator signature from the beginning.

287 If the Meter Systems includes displays with personal information it should be setup in a 'privacy by default' way – i.e. authentication should be required before the data shown on the display.

EG2.M.1 Because logical components of Smart Grids may be incorporated in different physical devices the guidelines should focus on requirements for the logical infrastructure. MID relevant devices like smart meters will play an important role in a real infrastructure but their architecture is currently focused on MID or national conformity only. The Measuring Instruments Directive 2004/22/EC (19) provides the necessary requirements for smart meters and other measurement components.

4.2. European Smart Metering Requirements

288 Today smart metering roll-outs are being implemented in different ways in different Member States and different actors are responsible for smart metering. Therefore a standardised set of services and architecture defined by the EU would be highly beneficial for an efficient implementation throughout Europe.

289 Starting with the smart metering functionalities, a number of high-level use cases are being developed at EU level, recognising these can be further analyzed into more detailed use cases as required. Those high-level use cases (as currently defined) which are relevant to Smart Grids (in whole or in part) include:

- Meter interface to home communications systems.
- Meter interface to sophisticated energy management systems.
- Customer display unit receiving messages from e.g. the network operator.
- Communication related to multiple-rate tariffs within the meter: setting of tariff schedules.
- Demand side response made available by customer.
- Demand side management by network operator (or supplier) as agreed by customer.
- Remote power limitation.
- Remote connection/disconnection: local disconnection when emergency load exceeded.
- Remote configuration: parameters for local generation set by network operator.
- Monitor meter system status: routine communications checking.
- Monitor diagnostics of electrical components: detection of inconsistent metering results.
- Monitor supply disruptions: provision of information on supply interruptions.

290 To balance demand and supply, new pricing schemes need to be developed like time of use and dynamic pricing. Pricing information needs to be available for residential customers on their information display.

291 To get a complete overview of the functionality of smart meters and its standards, a repository of business functions between actors in the smart meter value chain translated into use cases should be developed. EG2 advises to stimulate the development of a European repository of smart meter business functions, use cases and associated technical standards called European Smart Metering Requirements (ESMR), developed by the already existing Smart Meter Coordination Group (SMCG).

292 The scope of the work should include the various Technical Committees of the ESOs like equipment for electrical energy measurement and load control (CLC/TC13), communication systems for meters and remote reading of meters (CEN/TC294), and Home & Building Electronic Systems (HBES) (CLC/TC205).

293 A common European reference (the ESMR) will serve many goals. It will streamline the development of standards, ensures interoperability, can be used by Member States as reference material preventing duplication of work, it helps suppliers of smart meter hardware and software, and it creates a European level playing field and maximises economies of scale. It can be used as references when drafting international tenders and contracts. And finally, ESMR has the potential of removing the significant delays and costs of multiple testing and approval, allowing industry to be faster and cheaper to market with its products.

294 An inventory of the high level use cases at EU level and the existing use cases of Member States is a first step. The first version of the ESMR with detailed descriptions should be ready by the summer of 2011.

EG2.M.2 The European Smart Meter Requirements (ESMR) provide a good basis for technical requirements for meters and other Smart Grid components. It is recommended to further develop the ESMR in order to set up a technical standard for Smart Metering devices, and to consider introducing similar requirements for Smart Grids.

Appendices

A. Introduction to Smart Grids

295 The Smart Grid is an electricity grid that uses two-way ICT technology to optimise supply and demand. In addition to this it aims to increase the security of supply to the customers. Implemented in the right way it promises improved reliability by enabling quicker and more effective response to outages, greater customer awareness of energy usage and costs, and facilitation of the adoption of new technologies such as renewable generation sources and electrical vehicles. A Smart Grid is utilising digital technology. It overlays the ordinary electrical grid with an information and net metering system, which includes smart meters. Smart Grids are being promoted by many governments as a way of addressing energy independence, global warming and energy resilience / emergency issues.

296 Smart Grids are made possible by applying sensing, measurement and control devices with two-way communications to electricity production, transmission, distribution and consumption. Smart Grids communicate information about grid condition to system users, operators and automated devices, making it possible to dynamically respond to changes in power grid condition.

297 Included in the Smart Grid is an intelligent monitoring system that keeps track of all electricity flowing in the system. There is also the capability of integrating renewable electricity resources from solar and wind sources as well as switching to other modes of generation such as local power production. When power is least expensive the customer can allow the Smart Grid to turn on selected home appliances. Also factory processes that can run at arbitrary hours can be started by the grid. At peak times the grid could turn off selected appliances to reduce demand.

298 A Smart Grid employs innovative products and services together with intelligent monitoring, control, communication, and self-healing technologies in order to:

- enable the current electricity grid to handle decentralised volatile electricity generation on all grid voltage levels in a sustainable way;
- significantly reduce the environmental impact of the whole electricity supply system;
- allow customers to play a part in optimising the operation of the system;
- lower the CO_2 emissions of the energy supply chain, in production and consumption;
- provide customers with more detailed information and options for how they use their supply;
- help customers to reduce their energy consumption;
- better facilitate the connection and operation of generators of all sizes and technologies;
- facilitate Demand Side Management to better manage power demand, particularly as renewable sources of energy are deployed;
- facilitate Smart Grid beneficial shifts in the modality of energy generation resources at the local level;
- maintain or even improve the existing high levels of system reliability, quality and security of supply;
- foster market integration towards a European integrated energy market.

299 Next to these benefits, the Smart Grid also includes challenges, such as cyber security and the possibility of remote control of appliances within the home, the joint responsibility for supply by a large set of competing organisations, and the need for the regulatory framework to adapt while fostering both economic and security issues. The challenges include keeping up resilience and robustness of the Smart Grid, with the ability to keep

up its indispensable core functionalities (i.e. delivering electricity / energy). This should be the case even under crisis conditions, at least at the same level demanded of the current electricity grid.

300 Smart Grids thus encompass a much wider area than smart metering. Smart metering is an important first step towards a Smart Grid. Smart meters bring intelligence to the 'last mile' between the grid and the final customer. Without this key element, the full potential of a Smart Grid may not be realised. Being that only few countries in Europe have undertaken a full deployment of smart meters actors involved in the sector should draw from existing experiences and take account of best practices in place.

301 Other areas need to be addressed in parallel. One is the continuous development of the electricity grid's ability to electrically maintain the balance of electricity generation and consumption in a way compatible with the electrotechnical properties of the grid. This is getting a more and more complex task. In addition to smart metering, any thinkable sustainable solution for the complete change to renewable and sustainable energy sources; i.e. they will require a smarter layout of the large scale and local electrotechnical functionalities of the grid infrastructures as well as smarter ICT-based solutions - decentralised and within the critical operational core of the grids.

302 The course of Smart Grid adoption in Europe is far from clear. The underlying technologies remain expensive; their business case relies on assumptions of significant changes in customer behaviour; and cost-effective integration of existing systems and emerging technologies is not yet proven. The business model in many cases is still emerging, especially for customer applications, as regulators, utilities and third-party service providers define their roles and set technology standards. Many core systems remain unproven and currently a limited number of Advanced Metering Infrastructure (AMI) systems have been deployed in Europe.

303 There are some challenges and uncertainties for Smart Grid deployment. These are mainly dealing with cyber security and data protection (from a consumer perspective) and actual savings and costs (from a deployment perspective). Therefore, efficient measures safeguarding consumer protection should be in place before Smart Grids and smart meters can be deployed. In particular, the security of the Smart Grid and its susceptibility to hacking and attack need to be ensured. Also for the likely introduction of new energy deals which involve networks or suppliers remotely controlling appliances within a customer's home to help balance the power grid. While new deals may offer benefits such as lower cost tariffs to customers who participate, careful consideration will have to be given to the protections needed around these innovations.

304 The development of Smart Grids will be facilitated by the wide-scale deployment of electricity smart metering, as envisaged in 3rd Energy Package, directive 2009/72/EC (31). The complete Smart Grid deployment is a gradual evolution, not a 'roll-out' revolution.

A.1. Roles and responsibilities

305 The implementation of Smart Grids will be made possible by the participation of actors, according to their specific roles and responsibilities which are described in greater detail in the report by Expert Group 3 (17).The different roles and responsibilities are listed below.

A.1.1. Transmission System Operators

306 Transmission System Operators (TSOs) manage the high-voltage grid, 110 kilovolt (kV) and higher. 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.

307 Directive 2009/72/EC identifies the responsibilities of transmission system operators (TSOs), including the submission to the regulatory authorities of a non-binding Community-wide 10-year network development plan, every two years. Regulation EC 714/2009 (32) mandates TSOs to cooperate at Community level through the ENTSO for Electricity. Among other tasks, the ENTSO-E shall elaborate network codes for cross-border network issues and market integration issues interfacing with the power system users, EU institutions,

regulators and national governments. As far as harmonisation and standardisation are concerned, these areas include data exchange rules and interoperability rules.

308 The three key challenges for the TSOs are:

a) to optimise interconnection capacities;

b) to support the integration of large generation such as the large wind generation plants;

c) to keep the power grid stable and balanced in cooperation with the DSOs and neighbouring TSOs.

A.1.2. Distribution System Operators[74]

309 Distribution System Operators (DSOs) are responsible for energy distribution in medium and low voltage grids. Often DSOs are also the specialists when it comes to complex private energy grids and installations. The current role of being the data hub[75] for metering data will be extended by the task to manage an active power grid network that interacts with Renewable Energy Source (RES) and Distributed Generation (DG). Rather than conventional investments in 'copper', investments in enabling the power grid with ICT solutions will be necessary. However, considering the aging European infrastructure, Smart Grids will not remove the need for significant DSO investment in traditional network renewal in the next years. Tasks of DSOs include:

- **Active network management**: 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 customers' metrological register(s) for all information needed for network management and quality of supply management. This information should be shared on an as needed basis to fulfil regulated duties with service providers like DG operators and aggregators.

- **Local load management**: 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.

- **Electricity storage**: the storage of electricity can help to reduce load fluctuations, but can also be attractive for price arbitrage over time. DSOs can operate a storage facility and offer storage to energy suppliers and other DG-operators.

310 In distribution, with massive deployment of 'conventional' Distributed Generation 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. It follows that the DSO in the future will be interacting more frequently than today with TSOs, suppliers, generators and market operators. The future interfaces required to accomplish this will need to be specified in further detail[76].

311 The DSOs need to fulfil their duty in relation to the overall power grid stability and operational security, given that more and more distributed generation will be connected to the distribution grid. The data collected by DSOs is needed to facilitate an increasingly more dynamic distribution system because of:

a) growing distributed generation;

b) active management of demand;

---

[74] This does not fit with the UK smart metering model. In the UK, energy suppliers will be primarily responsible for reading customer meters, either directly (today) or via a central data communications company (in future). Networks do not read meters themselves, save in limited circumstances.
[75] DSOs are not a data hub in the UK.
[76] More details can be found in the report from Expert Group 1: Functionalities of Smart Grids and smart meters (21)

c) local storage;

d) electric vehicles (EV).

312 As more fluctuating distributed generation will feed into the distribution system, gathering and handling the data about the state of the distribution system will be a key issue for the DSO. In order to cope with the above challenges, the DSOs will have to continue upgrading their power grid infrastructure and control centres and need to keep educating their employees accordingly.

313 Regarding the interfaces among the actors, the need of a market role 'neutral and transparent information hub', for enabling demand response strategies need to be emphasised. The actual implementation of this hub is dependent on the national market model and may be adopted by several actors, such as DSOs.

314 The TSOs will have to provide more support & communication of data to the DSOs, but will also require more specific information from the DSOs, especially with more distributed generation coming from the distribution grids. TSOs need to forecast the overall system load in conjunction with the DSOs. At the same time, the DSOs will have to strengthen their role in providing the required data relating to the distributed generation, active management of demand, local storage and electric vehicles within the distribution grid.

315 It follows that TSOs and DSOs must significantly enhance the exchange of information and coordination, embracing activities such as power flow management, voltage control, alarm surveillance and fault management in order to be able to maintain a reliable and stable system at all levels of operation.

A.1.3. Energy Generators

316 Today, bulk power generators are responsible for supplying the major share of the load, for supplying ancillary services, black start and reserve capacity, as well as for contributing to voltage control. 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.

317 Europe is promoting renewable energy use in electricity generation. Therefore the EC issued directives on electricity generation from Renewable Energy Sources (RES). These are officially named Directive 2001/77/EC (33) and Directive 2003/30/EC (34) popularly known as the RES Directives. These directives however are amended and subsequently repealed by Directive 2009/28/EC (35) on the promotion of the use of energy from renewable sources.

318 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 (35).

319 Micropower Production (MPP) may augment the generation capacity as local power production. In case peak shaving is needed, the Smart Grid may initiate MPPs to generate power locally from e.g. gas or even temporary draining upon car batteries.

320 Some of the most effective tools by which the community can reduce its dependence on imported oil in the transport sector are increasing technological improvements (such as energy efficiency technologies), incentives for the use and expansion of public transport and the use of renewable energy sources in transport. As the security of oil energy supply is most acute, this may largely influence the fuel market for transport (35).

321 In order to reduce greenhouse gas emissions within the Community and reduce its dependence on energy imports, the development of energy from renewable sources should be closely linked to increased energy efficiency (35).

322 The European Commission monitors the Member States' progress and will, if necessary, propose mandatory targets for those who miss their goals. These EU targets already have impacts on generation. In some EU countries RES based generation has become not only an issue of investors but also of public interest.

Governments have started strong incentives which result in private entrepreneurship with mainly photovoltaic solar power (PV) based systems as well as mid size RES park operators with PV, wind and biogas generation[77].

A.1.4. Energy Market Suppliers

323 Energy market suppliers are responsible for supplying customers with their energy, for procuring that energy from their own sources and/or the wholesale market, for billing and serving customers. 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 customers, as well as other forms of assistance to customers, such as in paying their bills. Particularly in the context of Smart Grids, energy suppliers are one of the wider number of participants that include TSOs, DSOs and generators.

324 Energy market suppliers may also play a key role in demand side management. They can help to ensure that different types of customer are incentivised to consume energy at different times of the day or week, thereby enabling a smoother demand curve. This will become increasingly important as the energy mix changes to include more renewable sources of energy, which do not produce energy as consistently as current sources of energy like gas or coal fired power stations. DSOs will not always be able to manage this or have access to the data on individual customers and so will not know which consumers or types of customer they should seek to incentivise changes in consumption. It should be noted that the DSO is often not a party in the contract between consumer and company.

A.1.5. Metering operators

325 The metering operator is the entity which offers services to install, maintain and operate metering equipment related to a supply. In most EU Member States the DSO is also the Metering Operator. In case of a specific contractual basis, the contract is mostly with the network operator, or may be with the customer or the supplier. The meter may be rented to, or exceptionally owned by, the customer. In a few Member States, energy suppliers or independent metering companies are responsible for installing, maintaining and operating metering equipment.

326 Independent organisations or energy suppliers (like in the UK) can be responsible for reading meters and managing the metering infrastructure used by their customers. Metering operators and energy suppliers may need to obtain consumption information about their customers via the metering infrastructure as is necessary to deliver these functions. Micropower and independent power producers (IPP) may acquire data on energy produced and delivered to the power grid via the AMI.

A.1.6. Customers

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

- **Industrial customers**: a large customer of electricity in an industrial or manufacturing industry. These customers 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 customers**: residential customers of electricity (including agriculture users), which may be involved in contract-based Demand/Response.

328 The transition towards a decentralised energy concept reflects in at least two 'new' types of home customer:

- **Customers without the option of producing energy but with a potential to save energy**. This will be achieved by optimisation of the house infrastructure or by means of smart living concepts. Both need to be pushed by incentives as they are costly and a high percentage of customers may not be

[77] 'The achievement of the objectives of Directive 2009/28/EC requires that the Community and Member States dedicate a significant amount of financial resources to research and development in relation to renewable energy technologies. In particular, the European Institute of Innovation and Technology should give high priority to the research and development of renewable energy technologies'.

able to afford it. Smart living may leverage large and small potentials to save energy in households if customers invest in new smart devices and use of added value services for the individual private comfort zone. So smart living can provide the needed level of automation and reduce heavy human interaction.;

- **'Prosumers' with decentralised generation**. 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 his DG. Alternatively he can act as a micro or individual power producer (MPP or IPP) on the basis of a contract with his local DSO.

329 Home applications enabling demand side response have to be developed, including the 'smartness' of metering to inform the customers. Many appliances continue to draw a small amount of power when they are switched off. These standby power loads occur in most appliances that use electricity, such as televisions, stereos, computers, and kitchen appliances. Energy saving devices or devices that offer a real off switch can intelligently cut all power to these appliances. Home automation sensors, switches and controllers can be used to handle more complex sensing and switching. The potential benefits of smart meters will be different between consumer groups. It should be recognised that some consumers will not be able to fully use the benefits of smart metering, which may influence the willingness to adopt these meters.

330 To facilitate customer demand side response, standard customer load profiles used will be replaced by 'dynamic' load profiles in case of flexible energy prices and / or power grid tariffs. A change of standard load profiles will be needed for customers that actively manage their demand. These new load profiles should help retail suppliers to optimise their procurement from the energy market. In addition, energy suppliers will be more and more confronted with supplying customers that produce some of their own electricity.

331 In relation to customers' demand side response and to the growing importance of the power grid users who are both, producing and consuming electricity, adequate tariff structures will need to be elaborated taking into account energy (kWh), load (kW) and time of use, so as to ensure fairness towards all power grid users and adhering to the principle of causality.

332 The emergence of more dynamic energy pricing being offered by suppliers/retailers to customers is expected. These products may vary the price offered based on time-of-day or day-of-week related to the cost of electricity on the marketplace at that time.

333 Based on the increased information on consumption, customers should be better placed to make more informed decisions on how and when they can save energy, either by changing their behaviour or by engaging with an energy efficiency services provider.

334 Customers must have the choice whether other responsible parties than the DSO (or in some countries, such as the UK, their energy supplier) should have access to their specific energy usage data with a granularity of more than monthly / yearly (e.g. interval data, such as hourly). 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 customer. The type of control and the manner in which it is offered will need to be determined by the Member States. Moreover, the customers must have free access to their energy consumption data in a format that will help them compare offerings in the market. They must have the choice and control to share their own energy consumption information with such third parties[78] in order to benefit from the choice that competition offers in the market in terms of price, products and services. To that matter, all legal provisions for data protection and privacy must be complied in full. Moreover, energy providers need to seek specific and informed consumer consent to be able to use personal data for other than for legal duties.

335 Compatibility of in home technology including energy management systems, communications networks and smart meters is an important aspect for customers. Customers should be able to switch energy companies without having to change their display or other in-home smart products or services. Failure to address this would result in increased inconvenience to customers, barriers to competition, additional cost of purchasing new equipment and environmental waste from obsolete technology which is thrown away.

[78] The term 'third party' is used in this context to identify any individual and/or organisation and/or legal entity other than the DSO and who is not a party in the DSO's legal transaction but who might be affected by it.

336 Smart meters should not be able to be rolled out in Member States before this issue is resolved as this would result in increased cost to consumers (from stranded assets), inconvenience for customers who have to have their meters replaced when they switched provider and barriers to competition. This can be achieved by defining a standard for the interface between in home devices and meters.

337 Smart Grids can provide new services to customers. Examples of these new services to customers range from home automation devices, home energy management devices and services and data (mining) systems to enable identification of new customer opportunities, through contract based products to customers based on their individual usage pattern of energy. Customers will increasingly produce electricity too, and in case of surplus, they want the highest possible yield (buy low, store, sell high).

A.1.7. Energy Market Place

338 The flexibility of generators, customers and those that do both will create liquidity in local market segments at the distribution level. One can say that growing distributed generation implies higher flexibility but also increases volatility. It requires balancing supply and demand lower in the power grid using new forecasting concepts and tools. Some important developments effectuated by Smart Grids are listed below. It also requires the security of market information and a governance structure (strict rules and controls) to early detect and counter energy market instabilities and related instabilities in energy supply. This may be caused both by software, technical ICT failures, and deliberate energy market manipulation by criminals[79]

- **More Distributed Generation and higher flexibility and volatility**: Growing distributed generation poses operational and control challenges for the traditionally designed and operated distribution grids and is one of the key drivers for Smart Grids. It increases both flexibility and volatility.

- **Balancing supply and demand lower in the power grid**: Connection of distributed storage and micro generation to the medium and low voltage level networks will provide more options for the DSOs to balance their power grid areas, thereby reducing stress at the TSO level. Peak-shaving at the DSO level may reduce investments needed at the TSO level to cope with peaks of high demand. Important instruments are flexible energy prices, flexible power grid tariffs and their impact on the interfaces between customers and producers. Studies and early experience will need to reveal efficient ways to communicate with customers, such as e-mail, SMS, signals to the meter, in-home display, in-home energy management system, digital TV etc. From the overall energy efficiency respect the more local the balancing of the network, the less net-losses are incurred in the overall flow of energy. Hence local balancing is preferable.

- **All parties to develop forecasting**: Intraday trading will become an important instrument. More transparent and adjusted balancing & reserve power rules agreed between TSOs will be required, also in order to facilitate the development of cross-border intraday, balancing and reserve markets. Moreover, all players, including DSOs, suppliers, generators, Balance Responsible Parties, but also regulators will have to establish an appropriate forecasting framework and systems to cope with higher flexibility and volatility in the electricity supply chain. From this perspective, the application of state-of-the-art forecasting tools together with larger balancing areas are the key to integrate large amounts of variable renewable energy generation, e.g. from PV or wind power generation in a cost-efficient way.

A.1.8. Providers of Technologies, Products and Services

339 A Smart Grid ecosystem will consist of many service providers. The following technology solutions are generally considered when a Smart Grid implementation plan is developed:

- Advanced Metering Infrastructure (AMI);
- Customer Side Systems (CS);
- Demand Response (DR);

[79] Cf. (54) and (55).

- Distribution Management System/Distribution Automation (DMS);
- Transmission Enhancement Applications (TA);
- Asset/System Optimisation (AO);
- Distributed Energy Resources (DER);
- Information & Communications Technologies Integration (ICTI).

340 The innovation towards Smart Grids may be organised in public/private partnerships. In order to get the most effective and efficient solutions, TSOs, DSOs and energy suppliers are keen to make use of an innovation network with competing service providers for power grid specific services.

341 Providers of technologies, products and services have been classified into the following categories:

- Electric Power Grid Equipment manufacturers and their suppliers;
- Ancillary Services providers;
- Metering Operators;
- Information & Communication Technology (ICT) service providers;
- Smart Grid communications network providers;
- Building Automation / Energy Management providers;
- Smart home appliance manufacturers (e.g. white goods, heating devices);
- Electric Transportation / Vehicle Solutions providers.

A.2. The value of Smart Grid applications

342 Smart Grid applications can be grouped into three broad categories: advanced metering, power grid applications, and customer applications. These categories can all bring value to the actors in the Smart Grid infrastructure.

343 Some important Smart Grid developments are demand side response, demand side management and storage:

- **Demand Side Response** (by FERC[80]): Changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardised.

[80] The Federal Energy Regulatory Commission, or FERC, is an independent U.S. agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC also reviews proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines as well as licensing hydropower projects. The Energy Policy Act of 2005 gave FERC additional responsibilities as outlined in FERC's Top Initiatives and updated Strategic Plan. As part of that responsibility, FERC:

- Regulates the transmission and wholesale sales of electricity in interstate commerce;
- Reviews certain mergers and acquisitions and corporate transactions by electricity companies;
- Reviews the sitting application for electric transmission projects under limited circumstances;
- Licenses and inspects private, municipal, and state hydroelectric projects;
- Protects the reliability of the high voltage interstate transmission system through mandatory reliability standards;
- Monitors and investigates energy markets;
- Enforces FERC regulatory requirements through imposition of civil penalties and other means.

- **Demand Side Management** (from EIA[81] DOE[82]): The planning, implementation, and monitoring of utility activities designed to encourage customers to modify patterns of electricity usage, including the timing and level of electricity demand.

- **Storage** refers here to all forms of energy storage (e.g. chemical, kinetic, thermal). The energy stored can either be transformed into electricity or be used in the form in which it was originally stored (i.e. as pressure or steam). Future possibilities could possibly extend to batteries of electrical cars connected to the grid. It is therefore possible that electrical cars will play a substantial role in storage in the future, but the realisation might be extended until and beyond 2020. The interfaces required between the 'storage owners' and the network operators will require further analysis.

A.2.1. Advanced metering

344 AMI, also referred to as 'smart metering', consists of digital electricity or gas meters equipped with bidirectional communication capabilities that will enable energy providers to offer new tariffs and service providers to add value added services on top. For utilities a Smart Meter will make operational tasks more efficient. Smart Grid meters will also be the basic tool for the DSO to be prepared for future needs in Smart Grids. The direct benefits as of today includes, but is not limited to:

- Consumer benefits, such as automated meter reading (meaning bills are accurate and no longer estimated), new tariffs (e.g. time of use tariffs), more information on energy usage helping consumers to understand their usage, better energy efficiency advice helping customers to reduce bills, more support when consumers are struggling to pay bills, no more visits from meter readers, and others.

- DSO and supplier benefits include reducing operating costs (e.g. from not having to employ meter reading agents), the ability to fix meters remotely, the establishment of capabilities necessary to develop demand side management, the ability to forecast, hedge and purchase energy more efficiency, improved customer service and new ways to communicate with customers.

- Functions to operate Smart Grids. Smart Grid meters are sensors with measuring capabilities such as voltage etc. Smart Grid meters will help identify and resolve power grid relevant problems.

- Eased remote termination, limitation and reconnection of energy supply in case of defaulting payment by the customer (with a switch-off option implemented).

A.2.2. Smart Grid applications

345 The increasing amount of Distributed Generation (DG) at various levels of the energy infrastructure urge power grid operators to gradually change their monitor and control paradigm from top-down to bottom-up. Traditional operation practices do not suffice anymore. DG technologies introduce bottom-up energy flows and

---

[81] The U.S. Energy Information Administration (EIA) is the statistical and analytical agency within the U.S. Department of Energy. EIA collects, analyzes, and disseminates independent and impartial energy information to promote sound policymaking, efficient markets, and public understanding of energy and its interaction with the economy and the environment.

[82] The Department of Energy's (DOE) overarching mission is to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex. The Department's strategic goals to achieve the mission are designed to deliver results along five strategic themes:

- Energy Security: Promoting America's energy security through reliable, clean, and affordable energy;
- Nuclear Security: Ensuring America's nuclear security;
- Scientific Discovery and Innovation: Strengthening U.S. scientific discovery, economic competitiveness, and improving quality of life through innovations in science and technology;
- Environmental Responsibility: Protecting the environment by providing a responsible resolution to the environmental legacy of nuclear weapons production;
- Management Excellence: Enabling the mission through sound management.
-

tend to be less predictable. All network elements will involve monitoring, controlling, and automating operation of the distribution and transmission networks by means of secure information exchanges.

346 Matching supply and demand: The match between supply and demand has to be dealt with at a local level. It affects the energy market, but also the use of power grid capacity. It concerns both industrial as well as residential customers and will lead to more sophisticated tariff schemes and real-time data interchange.

347 Two areas of power grid operation that are affected are:

a) the provision of power grid stability and fault protection;

b) the continuous match between supply and demand.

348 Both will have to be dealt with at a local level. Grid stability and fault protection focus on short term data exchange in the range of tens of milliseconds

349 All network elements will involve monitoring, controlling, and automating operation of the distribution and transmission networks by means of a secure information exchange. The five applications that provide the most benefit to the power grid are:

- Volt-Var Optimisation (VVO) and Conservation Voltage Reduction (CVR). A network of sensors and intelligent substations should interact with DG systems. Additionally tap changers and reactive loads such as inductors and capacitor banks help to control the voltage level and power factor throughout the power grid. These technologies permit respond to conditions of the power grid also when market driven Distributed Generation affects the physics of the power grid.

- Fault Detection, Isolation and Restoration (FDIR), enable the DSO manually or automatically to reconfigure the power grid remotely in response to unplanned or planned outages by means of intelligent substations that include fault sensors and mid-circuit reclosers and ties.

- Wide Area Measurement (WAM) provides real-time and historical information about the state or predicted behaviour of the transmission grid using a network of precisely timed monitoring devices variously called synchrophasors or phasor measurement units (PMU's). A DSO will be enabled to steer the complete grid on behalf of TSO requirements. WAM also reduces the likelihood of major cascading blackouts.

- Field Area Measurement (FAM) Remote substation and feeder Monitoring and Diagnostics (M&D) can provide a wealth of nearly real-time operational data about substation and feeder equipment. New data and historical data can be used quickly to address impeding failures, or allow preventive rather than corrective maintenance and avoiding collateral damage.

- At the DSO and TSO-levels, shut Flexible Alternative Current Transmission Systems (FACTS) devices controlled by the Smart Grid will become important in controlling the reactive power flow in the smart energy grid. Static VAR Compensators (SVC), Thyristor Controlled Series Compensators (TCSC) and Static Synchronous Compensators (STATCOM) are examples of FACTS devices (36).

350 These applications could also be based on agreements between customer / building owner and grid operator for coordinated operation.

A.2.3. Customer applications

351 Smart Grid customer (consumer) applications or appliances like in-home displays, energy management equipment etc. focus on automated comfort or control services for customers (smart living or Demand Side Response – DSR – programs) or prosumers with Distributed Generation. Such devices will automatically shift demand from peak to off-peak times or produce energy on behalf of the customer (or – on longer term – even upon request by the Smart Grid local balancing application), with the requirement that these systems must be able to interact automatically with related signals. For households these signals may come from energy providers, service providers and/or the DSO.

352 Future customer applications will also likely integrate electric vehicles, and more sophisticated energy management and energy storage systems. Effective combinations will provide customers with the transparency, tools and incentives needed to reduce the burden they place on their finance, the energy grid and the environment.

353 However, the customers, particularly the residential customers, currently remain reluctant because their perceived value proposition is not viewed by them as compelling. More work is needed to communicate the Smart Grid and smart meter benefits to the residential customers. When the societal benefits are understood by customers, their overall value proposition may be compelling enough to create the tipping point needed to sustain and even accelerate the transition that is currently underway in Europe. In order to help maximise engagement, effective protections are needed to ensure consumer confidence in new energy products and services.

B. Telecommunications

B.1. Smart Grids and communication networks

354 To achieve the potential benefits of Smart Grid, critical foundational technological platforms need to be in place and available. Smart Grid applications rely on the advances the Electric Power System and increased integration with communications and information technology. Telecommunications will be one of the key elements that make the grid smart alongside sensors and actuators for active monitoring and control and intelligence or computing power to process the monitoring and control data.

355 Telecommunication in a broader context is already seen as a mission critical factor in traditional grid networks and currently TSO's and DSO's already deploy dedicated grid communication networks typically for monitoring and protection purposes. The role and importance of communication networks is set to increase significantly to enable new applications such as demand response, distribution automation, integration of renewable energy and electric vehicles.

356 Historically these networks were largely purpose-build to support a single application (e.g. protection). This approach will not be economically feasible and overly complex to support the flexibility required by new innovative Smart Grid functions. New network and security technologies enable multi-service networks that will drive convergence of operational networks onto a common platform.

357 This common platform will need to meet excessively more demanding requirements though, largely due to the exponential increase of sensors and actuators and innovative new applications such as demand response and wide area situational awareness. Reliability will be important with estimates ranging from 99 percent to 99.999 percent level for demand response applications. The delay of a significant number of DR commands due to high latency would greatly impact effectiveness of the system. Situational awareness applications would pick up disturbances in the network and would provide operators a dynamic picture of the status of the grid. For example introduction of synchrophasor technology would significantly drive up bandwidth combined with low-latency requirements to support detection of local disturbances.

358 Grid communications network providers plan, build and maintain the communications systems that enable the data communication required to maintain grid stability, load balancing and fault protection systems by a TSO or DSO. This function is mostly executed by the TSO or the DSO, or may be performed by an independent actor but the overall responsibility and ownership of this technical information remains with TSO and DSO. The grid communications network provider ensures compliance with the agreed service levels (Service Level Agreements including quality of service, data security and privacy) and compliance with any national and/or international regulations as necessary.

359 Electricity generation and consumption must be balanced across the whole grid to ensure a continuous supply. The complication of integrating distributed generation in the form of millions of local domestic generators (DG) across Europe would create new challenges for energy network operators (TSO's and DSO's). To provide stability and quality of service in the networks of the future, control and management of many thousands of items of electrical plant, even within a single company, will be essential. This in turn will drive the widespread adoption of sensoring technology, specifically in the distribution network, needed to monitor grid status and loading.

360 A failure in any part of the grid can cause further failures, unless action is taken quickly. The current that is re-routed over transmission or distribution lines not having sufficient capacity can potentially lead to a collapsing information flow which triggers cascading failure and widespread outages. It is therefore essential to ensure continuity of supply, to monitor and control the complete grid network from power generation through transmission to distribution and support for islanding and microgrids. Reliable and efficient control mechanisms require a highly secure and resilient communications network that can support the applications needs of the different elements of the grid network.

361 As mentioned before, Smart Grid applications will be introduced gradually as technology matures, the regulatory framework develops and demand is put in place. The common denominator for most Smart Grid applications will be the network capabilities. It takes significant lead time to develop and implement a communications platform that is scalable, versatile, future proof and robust. One key requirement to support a future proof architecture is the adoption of open standards. With the internet in mind, the past has proven that networks (either public or private) with an architecture based on IP will meet these demands. Similarly in North America, IP is determined as a core technology of Smart Grid. At the same time, the weaknesses that the current generation IP (IPv4, on which Internet is based) and numerous commonly used communication protocols on top of IP (such as Telnet, SNMP, SMTP, FTP but also industrial protocols like Modbus) are facing, must be counteracted. This is partly consolidated in the IETF specification of the next generation IP (IPv6). This will provide a better platform for current and future services and growth. However an architecture based on either IPv4 or IPv6 will require enhancing security measures to ensure secure end-to-end connections for these services from one node to an arbitrary other node: a typical requirement for Smart Grids. Besides services, the IP architecture is also able to adopt a multitude of communication technologies (as long as they include an IP stack). While for some elements of the communications networks wired solutions may be feasible and suitable, in many other instances wireless is a necessity to provide the necessary flexibility and minimise costs.

362 Many communications and networking technologies can be used to support Smart Grid applications, including traditional twisted-copper phone lines, cable lines, fibre optic cable, cellular, satellite, microwave, WiMAX, power line carrier, and broadband over power line, as well as short-range in-home technologies such as Wi-Fi and ZigBee. Each technology will reliably support specific use cases and architectures, but real-world technologies will see combinations of technologies to support diversity and specific limitations.

363 Specifically wireless technologies hold much promise, but the development and adoption of this technology will depend on the availability and affordability of spectrum. Information provided by utility companies in Europe indicate that there is currently no harmonised spectrum to support their mission critical communication requirements. Instead, individual frequencies are typically assigned on a country by country basis for applications such as SCADA, PMR and backhaul links. There is currently insufficient spectrum available for the public sector (TSOs and DSOs) to meet their Smart Grid needs. Similarly to recent development in the US and Canada, access to sufficient harmonised spectrum would open up the market to innovation and economic development. In Canada dedicated spectrum was allocated to utilities to support grid reliability. The spectrum, harmonised across the different provinces is driving the development of utility-specific solutions.

364 Wireless technologies can be adopted that rely on unlicensed spectrum, but is potentially risky. Unlicensed means that the utility will not have exclusive use and this could lead to congestion, making performance potentially unreliable. License-exempt spectrum is therefore not regarded as a viable option for mission-critical applications. For less critical applications such as meter reading unlicensed spectrum could be an option.

365 The rollout of smart meters offers an opportunity to establish an alternative grid communication infrastructure. The most efficient wireless deployment model would require access to sub 1GHz spectrum that would support IP-based radio systems. The installed equipment infrastructure basis decreases significantly when deploying in lower spectrum bands. In the US many utilities are deploying wireless networks in the sub-900MHz bands. This model might not work exactly in Europe due to a larger meter density per transformer, but it does have merit for further evaluation. Many European utilities have access to small amounts of spectrum in the 400 – 500Mhz band. If elements of this band were made available on a harmonised basis, substantial benefits in the creation of competitive products, time to implement systems and to lower costs would result.

366 For Mission-critical applications, dedicated spectrum would be required to make wireless networks and option. Ideally utilities should be able to provide ubiquitous coverage across their service territory. They should be able to deploy 4G cellular (LTE, WiMAX) technologies to support current and future (10 year plus) applications. These networks will need to be secure (encryption, authentication), reliable (99,99%) and support low-latency.

367 The rollout of a utility network can potentially be coupled with the EU initiative for a digital communication agenda 2020 to support broadband access in rural areas. The important difference in the communication agenda and energy efficiency agenda is that the communication infrastructure develops from urban to rural

areas whereas rural areas already are and will be the core of DG and Smart Grids. Possibly synergies between deploying rural broadband and Smart Grid communications could lead to economies of scale and scope.

368 Of course, not all of the required Smart Grid communications applications need access to dedicated networks to meet the necessary high to very high reliability, cyber security and quality of service (24/7) requirements. For some less critical applications, it may be feasible to share networks (e.g. public cellular networks). Also, it may be possible to utilise capacity on fibre networks where there is a need for higher data rate fixed point-to-point communications. But for low capacity point to multipoint communications, especially in rural areas, wireless technology will be the most cost effective solution.

369 Environmental restrictions will not generally allow the use of high towers to provide clear line of sight so it is necessary to compromise and use frequencies that can operate over obstructed paths (and sometimes into basements). That is the reason why the utilities already have access in many European countries to spectrum in the range 415 to 465 MHz (e.g. in the UK 457.5 to 464 MHz is allocated to scanning telemetry). However in many cases it is also requested to have short-medium distance communications to reach dispersed plants through point to point and point to multipoint access techniques. For these applications microwave frequencies in the range of 2.4 GHz, 5.4 GHz as well as 11 GHz could be allocated.

B.2. Electro-magnetic Hypersensitivity

370 'Electromagnetic Hyper-Sensitivity' (EHS) or 'Electrosensitivity' is a set of claims of adverse medical symptoms purportedly caused by exposure to electromagnetic fields, a condition that has been investigated seriously. It is named 'Idiopathic Environmental Intolerance with attribution to electromagnetic fields' by the World Health Organisation (WHO). The symptoms attributed to Extremely Low Frequency (ELF) and RF fields are similar and in many cases the afflicted subjects report both ELF and Radiofrequency RF fields to trigger symptoms.

371 Health complaints described as EHS and reported to be triggered by mobile phones, video display units (VDUs) associated with computers and TV sets and likely in the future also by Smart Grids and the smart meter, have been studied in a limited number of provocation studies. World Health Organisation (WHO) Workshops on Electrical Hypersensitivity and recent reviews of the literature on subjective health complaints associated with electromagnetic fields and provocation studies including subjects reporting EHS have presented similar conclusions. The main conclusion is that although symptoms described as EHS are real and may be severe and disabling, a relationship between symptoms and Radiofrequency (RF) field exposure has not been proven.

372 So until now, as far as EG2 knows, scientific studies have failed to provide support for a relation between RF exposure lower than the reference values in the present International Commission for Non Ionizing Radiation Protection (ICNIRP) guidelines and self-reported symptoms (sometimes referred to as electromagnetic hypersensitivity). Available studies suggest that self-reported symptoms are not correlated to an acute exposure to RF fields, but the limited number of studies does not allow any firm conclusion.

373 The electromagnetic environment consists of natural radiation and man-made electromagnetic fields that are produced either intentionally or as by-products of the use of electrical devices and systems. The natural radiation is orders of magnitude below local field levels produced by man-made radio frequency RF-sources. Sources generating high levels of electromagnetic fields are typically found in medical applications and at certain workplaces. The everyday use of devices and systems emitting RF electromagnetic fields is continuously increasing.

374 For broadcasting high RF power is generally required to maximise the area of coverage. Close to the antennas electric field strengths can reach several hundred volts per meter. Even higher values can be found close to occupational sources used for processing of various materials by heating and sometimes by formation of plasma discharge in the material. In many such applications RF-safety problems arise because RF-power is high and it may be difficult to enclose the field-generating electrodes and processing space inside a good electromagnetic shield.

375 Sources used by the general public e.g. for wireless communication, data transmission or food processing generate comparably much lower fields at the position of the user. But this may also depend on the behaviour of the user especially concerning the distance to the source. Cellular mobile communication networks cause on average low levels of electromagnetic fields in areas accessible to the general public. Handsets and cell phones,

however, might cause significantly higher peak levels of exposure during use, especially when attempts are made to communicate with base stations at a distance (e.g., when adjacent base stations are disrupted). Electronic article surveillance (EAS) systems and radio frequency identification devices (RFID) operate at many different frequencies within the RF band. Inside some EAS gates electromagnetic fields could get close to the existing exposure limits. In general these systems cause only low fields in the environment.

376 Radars produce high power main beams only a few degrees wide and usually not accessible during operation. In addition radar antennas can rotate (or directed in the case of phased array radars) and signals are pulsed, leading to a reduction in average exposure.

377 Although studies did not provide any clear conclusions, we should not underestimate this risk. There are growing concerns internationally about the health risk associated with smart metering, especially in the U.S., where high wireless transmission power levels are used for the communication between smart meters and concentration node. There is a large volume of information available online, most of which is unlikely to reassure consumers, for example emotive claims of harmful effects on health (e.g. claims of increased health risk for toddlers, and comparisons of the electromagnetic fields of smart meters (in the home) with existing fears regarding telephone masts). While with other types of information on the internet, consumers are able to read widely, and draw their own conclusions as to which sources are reliable; this is unlikely to be the case here. This is a complex scientific issue which makes it very difficult for the majority of consumers to separate fact from fiction when researching online. In addition, there are a number of areas where it is admitted that there is not enough information. This should not be underestimated.

378 In some countries which have begun to rollout smart meters, there seems to be a significant level of public concern. In Fairfax, California high levels of public concern about the health effects of EMF radiation from smart meters (together with concerns about privacy) led to the Fairfax Town Council approving a six-month moratorium on the installation of Smart Meters, which began in August 2010. The rollout of smart meters has also been halted in Watsonville, California. The California Public Utilities Commission's Division of Ratepayer Advocates (DRA) has recommended: '... immediate [Public Utilities] Commission action to address concerns about RF interference and possible adverse impacts on health and safety.' It says that: '... the Commission would be remiss in its duty to ensure 'safe and reliable' service if it did not solicit further evidence and perform an analysis'. The California and Maine Public Utility Commission (PUC) announced that the local utility should develop an opt-out option for wireless smart meters. This option should be provided at low cost.

379 As mentioned, a relationship between RF/ELF field exposure and EHS symptoms has not been shown in scientific studies. From these results it seems clear that RF/ELF field exposure is neither a necessary nor a sufficient factor to trigger health complaints in individuals reporting symptoms. However, whether RF/ELF fields may be a contributing factor under some conditions remains to be determined. In these conditions, it is very difficult to find solutions for afflicted individuals. In any case, the issues regarding local conditions of exposure are under the competence of national authorities.

380 In 2008 the European Parliament adopted by 559 votes to 22, with 8 abstentions, a resolution on health concerns associated with electromagnetic fields (EMFs). Among others, the Resolution urged the European Commission to revise the scientific basis and adequacy of EC limits for EMFs, which date back to 1998.

381 The EU Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) adopted an opinion on Health Effects of Exposure to EMFs in January 2009. It concluded that exposure to radio frequency RF fields is unlikely to lead to an increase in cancer in humans. However, it is not clear what the long-term effects (i.e. exposure of more than ten years) could be: '... as the widespread duration of exposure of humans to RF fields from mobile phones is shorter than the induction time of some cancers, further studies are required to identify whether considerably longer-term (well beyond ten years) human exposure to such phones might pose some cancer risk.' However, it states that there is some evidence that ELF magnetic fields can cause cancer in humans but that: '....it is far from conclusive. This was concluded based on studies indicating that children exposed to relatively strong ELF magnetic fields from power lines were more likely to develop leukaemia than those exposed to weaker fields. These results have not been confirmed or explained by experiments on animals and cell cultures.' In terms of harm to the environment, SCHENIR concluded that: 'The current database is inadequate for the purposes of the assessment of possible risks due to environmental exposure to RF, IF and ELF fields.'

382 For studies of health effects on people exposed to RF fields it is clearly important to have meaningful estimates of exposure over time. Instruments have been developed to enable exposure estimates. This could include using personal exposure monitors worn on the body. The characteristics of these types of device is to carry out data logging over periods of activity that sample field strength periodically and store the results for subsequent downloading .

383 In some Member States customers have a free choice to accept the smart meter and if they move to a property with a smart meter, customers have a free choice to opt-out of smart meter electronic usage-data transfer. When a customer has chosen opt-out, no energy usage data will be electronically transferred. Invoicing remains to take place based on estimates and manual meter readings, also when a smart meter is installed. However, a smart meter will always have a minimum level of data communication to ensure its right functioning.

384 In case of demonstrated EHS, when also the opt-out minimum level of data communication is unacceptable, the customer can ask for removal of the smart meter, replacing the smart meter by a conventional meter, but restrictions may apply and vary per Member State.

Case: Transferring cost to consumers

On March 25, 2011 the information site metering.com read the following:

Pacific Gas and Electric Company (PG&E) has come up with a plan to give customers a smart meter opt-out option by having the radios in their smart meters turned off and being required to pay the costs of having their meters read manually.

Under the proposal, customers would pay reasonable upfront and recurring fees to cover the costs of turning off the radio, manually reading the meters every month, modifying IT systems and providing information to customers on the program through call centers and other channels. The fees would also help reinforce the existing SmartMeter™ network to compensate for any degradation that turning off the radio causes.

Customers enrolled in the California Alternate Rates for Energy program would receive a discount of 20 percent. Customers would also have the option to take advantage of reasonable financing plans on the upfront charge.

Additionally, customers who would like their smart meters moved to a different location on their property can request that, with the cost of relocating the meter depending on factors such as whether the customer receives underground or overhead service.

The costs for customers who choose to keep a fully functioning smart meter would remain unchanged.

“We believe this proposal addresses concerns some customers have about SmartMeters™ while still delivering the many benefits of the technology to the majority of customers,” said Greg Kiraly, PG&E vice president, SmartMeter™ Operations. “The overwhelming weight of scientific evidence assures us that the low level radio frequency signals from our SmartMeters™ are safe, but we know some customers nevertheless have concerns about the meters and we take those concerns seriously.”

PG&E yesterday submitted the proposal to the California Public Utility Commission. Once approved PG&E would work quickly to make the option available to customers, the company said in a statement.

The plan was submitted on the request of PUC president Michael Peevey, who in a surprise move on March 10, directed “PG&E to prepare a proposal for our consideration that will allow some form of opt-out for customers who object to these devices at reasonable cost, to be paid by the customers who choose to opt-out.”

So far no other utilities in the state have been asked to present opt-out plans, although activists in San Diego are starting to agitate for an opt-out option from San Diego Gas & Electric.

C. Relevant organisations

C.1. Legislation and research

C.1.1. EU Policy Plans

C.1.1.1. SET - Plan: Strategic Energy Technologies Plan (EU)

385 The SET- Plan is the technology pillar of the EU's energy and climate policy. The plan, adopted by the European Union in 2008, is a first step to establish an energy technology policy for Europe. It is the principal decision-making support tool for European energy policy, with a goal of:

- accelerating knowledge development, technology transfer and up-take;
- maintaining EU industrial leadership on low-carbon energy technologies;
- fostering science for transforming energy technologies to achieve the 2020 Energy and Climate Change goals;
- contributing to the worldwide transition to a low carbon economy by 2050.

386 Implementation of the SET-Plan started with the establishment of the European Industrial Initiatives (EIIs) which bring together industry, the research community, the Member States and the Commission in risk-sharing, public-private partnerships aimed at the rapid development of key energy technologies at European level. In parallel, the European Energy Research Alliance (EERA) has been working since 2008 to align the R&D activities of individual research organisations to the needs of the SET-Plan priorities, and to establish a joint programming framework at the EU level.

387 The projected budget for the SET-Plan has been estimated at up to €71.5 billion (public and private investments for research, development and demonstration projects). The SET- Plan has two major timelines:

- For 2020, the SET-Plan provides a framework to accelerate the development and deployment of cost-effective low carbon technologies. With such comprehensive strategies, the EU is on track to reach its 20-20-20 goals of a 20% reduction of CO2 emissions, a 20% share of energy from low-carbon energy sources and 20% reduction in the use of primary energy by improving energy efficiency by 2020.
- For 2050, the SET-Plan is targeted at limiting climate change to a global temperature rise of no more than 2°C, in particular by matching the vision to reduce EU greenhouse gas emissions by 80 - 95%. The SET-Plan objective in this regard is to further lower the cost of low-carbon energy and put the EU's energy industry at the forefront of the rapidly growing low-carbon energy technology sector.

388 **Transition to a low-carbon economy:** the European Union recognises the need to move towards a low-carbon economy. The EU Energy and Climate Policy set ambitious targets for all Member States. With comprehensive strategies such as the SET-Plan, the EU will reach its goals of a 20% reduction of CO2 emissions, a 20% share of energy from low-carbon energy sources and 20% reduction in the use of primary energy by improving energy efficiency by 2020.

389 The SET-Plan - the technology pillar of EU's energy and climate policy - aims to not only achieve these objectives, but transform the entire energy system: from the way we source and produce energy, to how we transport and trade it, to how we use it. Low-carbon energy technologies such as wind, solar photovoltaic and biofuels must be affordable and competitive to be fully integrated into the energy economy.

390 To support the SET-Plan, the mission of the Strategic Energy Technologies Information System (SETIS) is:

- to establish an open-access information system on energy technologies and their innovation aspects. This information is geared towards supporting effective strategic planning, monitoring and assessment of the SET-Plan;

- to develop an integrated approach for information and data exchange on energy technologies and capacities for innovation throughout Member States, international organisations and energy sectors.

391 **Technology Roadmaps:** the Technology Roadmaps are a basis for planning and decision-making, and define the European Industrial Initiatives (EIIs). These Roadmaps put forward action plans aimed at raising the maturity of technologies to a level that will enable them to achieve large market shares in the period up to 2050.

C.1.1.2. SETIS: Providing targeted support to the SET-Plan

392 SETIS is the European Commission's Information System for the SET-Plan led by the Joint Research Centre. It supports the strategic planning and implementation of the SET-Plan. It makes the case for technology options and priorities, monitors and reviews progress regarding implementation, assesses the impact on policy, and identifies corrective measures if needed. SETIS has two principal activities, which are based on its own transparent research:

- Technology mapping: key information on the status and prospects of low-carbon technology with respect to EU policy goals;

- Capacities mapping: an estimation of the current public and private research and development (R&D) expenditures across the EU-27 on the priority energy technologies.

393 SETIS has also developed an Energy Cost Calculator, which compares cost projections for different technologies. It also shows the main elements that contribute to the cost of production. This information can be readily used to analyze where strategic efforts should be targeted.

394 The Strategic Energy Technology Plan (SET-Plan) aims to increase, coordinate and focus EU support on key low-carbon energy technologies. Implementation of the SET-Plan began with the establishment of the European Industrial Initiatives (EIIs), which bring together industry, the research community, Member States and the Commission in risk-sharing, public-private partnerships aimed at the rapid development of key energy technologies at European level.

395 The six EIIs focus on data exchange on low-carbon energy technologies. They focus on technologies for which the barriers, scale of investment and risk can best be tackled collectively. The European Industrial Initiatives include:

- European Biofuels Technology Platform

- European Technology Platform for the Electricity Networks of the Future

- European Technology Platform for Wind Energy

- European Photovoltaic Technology Platform

- Sustainable Nuclear Technology Platform

- Zero Emission Fossil Fuel Power Plants.

396 In some sectors of strategic importance to Europe, European Joint Technology Initiatives (JTIs) are established, funded by the European Commission, along with Member States and industry. These are public - private partnerships implemented under the Seventh Framework Programme (FP7) for large scale initiatives. One has been set up in a SET-Plan energy field: Fuel Cells and Hydrogen (FCH) Joint Technology Initiative. Its aims are to deliver 'fit-for-use' hydrogen energy and fuel cell technologies developed to the point of commercial take-off.

397 SETIS provides support to EU policy-making and decision-making by developing science-based responses to policy challenges with a socioeconomic and a scientific/technological dimension. SETIS has four primary activities: Technology Mapping, Capacities Mapping, Technology Roadmaps and monitoring and review of the SET-Plan implementation.

398 **Industrial Initiatives**: In 2008, the Commission proposed to launch six European Industrial Initiatives (EIIs): Wind, Solar (both concentrated solar and photovoltaic), Carbon capture and storage, Electricity grids, Bio-energy and Nuclear fission. The launch of the first four EIIs took place at the Madrid SET-Plan conference in June 2010.

399 **EII Implementation Plans**: The SET-Plan High Level Steering Group asked all European Industrial Initiatives (EIIs) to develop an Implementation Plan. The implementation plans cover the first 3-year period and are revised every year, thus becoming rolling programs.

400 **Transition planning**: The SET-Plan proposed three main implementation instruments as a basis for an Energy Technology Policy for Europe. Alongside the European Industrial Initiatives (EIIs) and the European Energy Research Alliance (EERA), the 3rd implementation pillar relates to activities addressing future European energy infrastructure networks and systems transition planning.

401 **Key figures**: In support of the 2nd Strategic European Energy review (2008), SETIS calculated the production cost of electricity from a wide range of power generation technologies in 2020, based on a thorough assessment of their techno-economic characteristics and available forecasts for the price of fossil fuels and carbon dioxide.

C.1.2. EU Research Institutions

Name	**European Energy Research Alliance (EERA)**
Link	http://cordis.europa.eu
Structure:	In parallel with the EIIs, the European Technology Platforms (ETPs) has been working since 2008 to align individual research organisation R&D activities to the needs of the SET-Plan priorities, and to establish a joint programming framework at EU level.
Mission, goals and objectives	EERA helps to optimise EU energy research capabilities through the sharing of national facilities and the joint realisation of Member State and European programmes. It also intends to accelerate the development of new low-carbon technologies. EERA's objectives consist of: • to accelerate the development of new energy technologies by conceiving and implementing Joint Programmes of research in support of the SET-Plan priorities; • to work towards a long-term integration of pan-European energy research infrastructures ; • to strengthen Europe's capacity to initiate and execute large precompetitive high-risk high-gain research and development programmes; • to develop links and sustained partnerships with industry; • to develop training, education and outreach activities for new researchers and professionals in strategic energy sectors.
Additional information	-

Name	**Joint Research Centre (EC)**
Link	http://ec.europa.eu/dgndex.cfm?ids/jrc/i=10
Structure	The Joint Research Centre is the scientific and technical arm of the European Commission. It is providing the scientific advice and technical know-how to support a wide range of EU policies. Its status as a Commission service, which guarantees independence from private or national interests, is crucial for pursuing its mission. The JRC has seven scientific institutes, located at five different sites in Belgium, Germany, Italy, the Netherlands and Spain, with a wide range of laboratories and unique research facilities. Through numerous collaborations, access to many facilities is granted to scientists from partner organisations. The

	JRC employs around 2750 staff coming from throughout the EU.
Mission, goals and objectives	'The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.' In order to deliver the best support, the JRC focuses its efforts on seven thematic areas, which respond to major EU and global challenges and take into account the JRC's proven competences: • Towards an open and competitive economy • Development of a low carbon society • Sustainable management of natural resources • Safety of food and consumer products • Nuclear safety and security • Security and crisis management • Reference materials and measurements.
Additional information	The JRC takes part in research and technological development actions of the Framework Programs (FP) on the same basis as legal entities established in a Member State. The indirect actions complement the work carried out in the frame of the JRC's own work program and are an essential tool for acquiring and transferring expertise and know-how. The JRC collaborates with over 1000 (a large majority of which are located in the EU Member States) different research and other organisations - both public and private – and in about 100 institutional networks to achieve its goals. The JRC offers a huge variety of temporary and permanent work opportunities and training for scientific and technical staff. Collaboration with these partners takes different forms, for example: joint research projects, networks with national enforcement laboratories & agencies, knowledge transfer, opening up access to JRC large scale facilities and databases, participation in workshops & seminars, mobility & training schemes for young scientists, a targeted approach to integrate New Member States, Candidate countries and neighbouring countries. The JRC research programs are decided by the Council of the European Union and funded by the EU budget with additional funding from associated countries. Under the European Union's Seventh Framework Program (FP7) and the Seventh Framework Program of the European Atomic Energy Community (EURATOM), the JRC's multi-annual work program is organised into five policy themes for which the funding (2007 numbers) over the seven-year period of the Framework Program is as follows: • prosperity in a knowledge intensive society: € 683 million; • solidarity and the responsible management of resources: € 578 million; • security and freedom: € 403 million; • Europe as a world partner: € 88 million; • the EURATOM program: € 517 million. These themes are further sub-divided into a total of 17 policy agendas that cover specific EU policy objectives - and which draw on the integrated expertise of our seven Institutes and their research partners. The continued solid funding through successive framework programs reflects the strong support for the work of the JRC by both the European Parliament and a broad spectrum of Member States. They also encourage the JRC to participate in all indirect actions of FP7 and recognise the important role it plays in research training, as well as the relevance to the European Research Area (ERA) of its extensive facilities for reference measurement and fundamental research. The non-nuclear part of the JRC program is steadily growing, and now constitutes about three quarters of the JRC's overall activities. This work is focused on research topics of particular relevance to European policy, with a new emphasis on understanding the relationship between environment and health, the increase of internal and external security, and support to the Lisbon process. Nuclear activities continue to account for just over a quarter of the workload. They support the whole range of research actions carried out in trans-national cooperation in the thematic areas of nuclear waste management and environmental impact, nuclear safety and nuclear security. The JRC's energy-related activities, conducted in the context of the EU's aim for an Energy policy for Europe, focus on sustainability of energy production systems - in particular, new and renewable energy sources - security of supply and competitiveness. • Energy Systems Technology Modelling (SYSTEM) The first core activity of the SYSTEM Action is to study the current and future prospects of low carbon energy supply and demand technologies and their impacts and interactions within the future EU energy system as they advance from concept to commercial applications. To do so, it focuses on developing and using analytical tools and models produced in-house and/or commercially available for techno-economic energy technology evaluation and assessment of their associated impacts on the key EU Energy policy

	drivers. In parallel, efforts are undertaken to develop competence to investigate the necessary transition of energy infrastructures and its requirement in terms of planning for shifting from today's energy system to a more sustainable European energy system. SYSTEM outcomes strongly feed into the Technology Mapping function of the Information System of the SET-Plan (SETIS), which aims at providing sound and robust information and knowledge on low carbon technologies to the SET-Plan Steering Group for decision making. The second core activity of the SYSTEM Action is to facilitate the collection, disseminate and render accessible information on energy technologies that is produced by SETIS to all interested stakeholders, especially, the European institutions, the EU Member States and relevant international organisations (e.g. IEA). To do so, the Action develops and operates energy technology related databases and runs the web portal infrastructure of SETIS. The SYSTEM Action collaborates with other JRC Actions, with other services of the Commission, and with its developed network of experts in international associations and organisations in the Member States. The Action interacts strongly with European and international research capacities on energy technology modelling and databanks. The Action contracts also external experts to obtain specialised information, whenever that is deemed necessary. • SES- Security Of Energy Systems (SES) The SES Action will be a new action within the framework of the new Energy Security Unit. The priority of the Action for this first year of activity will consist in the development of internal competences on selected aspects of the multidimensional topic of energy security and in starting to set up and/or to familiarize with a pool of quantitative tools especially useful to support the customers DGs in their policy needs. In practice, the Action will focus on the development of a GIS (Geographical Information System) based database for the EU energy systems infrastructures and of a set of quantitative models dealing with the energy systems on an EU scale. Methodological tools for assessing carefully selected specific aspects of energy security, namely infrastructure risk assessment and external cost evaluation, will be also acquired in order to complete the investigation of the energy security concept initiated by the SOS action. • Assessment of Energy Technologies and Systems (ASSETS) In line with the mission of the Institute for Energy, the ASSETS Action aims to provide scientific and technical information (data and techno-economic analyses) on energy technologies and infrastructures in the areas of: • energy resource exploitation and transformation; • power and heat generation; • resource and power delivery; • end-use industrial applications. • sound policy decision making in energy related Commission initiatives with a special emphasis on the Information System of the European Energy Technology Plan (SETIS) and the Strategic European Energy Reviews. The JRC annual budget comprises €330 million, coming from the EU's research budget. Further income is generated through the JRC's participation in indirect actions, additional work for Commission services and contract work for third parties, such as regional authorities and industry. A portion of the JRC's income comes from participation in FP7 indirect actions, performing additional work for Commission services, and contract work for third parties such as regional authorities or industry. These activities complement the tasks outlined in the JRC's work program and are seen as an essential tool for acquiring and transferring expertise and know-how.

Name	**EIT European Institute of Innovation and Technology**
Link	http://eit.europa.eu/home.html
Structure	The EIT is a new independent community body which was set up to address Europe's innovation gap. EIT aims to rapidly emerge as a key driver of EU sustainable growth and competitiveness through the stimulation of world-leading innovation. The European Institute of Innovation and Technology (EIT) is to be a key driver of sustainable European growth and competitiveness through the stimulation of world-leading innovations with a positive impact on economy and society. In return, participating research and education organisations will benefit from the prestige and visibility of the EIT, increasing their capacity to attract the best possible talents ('brain-gain').
Mission, goals and objectives	The mission of the EIT is to grow and capitalize on the innovation capacity and capability of actors from higher education, research, business and entrepreneurship from the EU and beyond through the creation of highly integrated Knowledge and Innovation Communities (KICs). Knowledge and Innovation Communities (KICs) are innovative 'webs of excellence': highly integrated partnerships that bring together education, technology, research, business and entrepreneurship. The KICs will be driving effective 'translation' between partners in ideas, technology, culture, and business

	models, and will create new business for existing industry and for new endeavours. A strong component will be to educate and develop entrepreneurial people and enhance their ability to work across stakeholder boundaries. It is expected that the KICs will have a significant societal impact, not only through their thematic work, but also through the creation of a new culture of innovation in Europe. The KICs will promote the production, dissemination and exploitation of new knowledge products and good practices in the innovation sector, transforming the results of higher education and research activities into commercially exploitable innovation. The obligatory inclusion of the business and higher education dimensions will ensure a constant focus on delivering and disseminating usable outcomes. In view of its long-term development perspective, the EIT will follow a gradual approach in establishing the KICs. In the first phase, three KICs were established for a period of seven to fifteen years, in order to ensure mid- to long-term sustainability of the chosen partnerships. • Climate change mitigation and adaptation: Climate-KIC • Future information and communication society: EIT ICT Labs • Sustainable energy: KIC InnoEnergy
Additional information	The Governing Board is the principal driving force behind EIT governance issues and is independent and autonomous in its decision-making. It is entrusted with the role of strategic leadership and coordination of the EIT's activities and is responsible for the selection, evaluation and support of the Knowledge and Innovation Communities (KICs). The Governing Board brings together 18 high-calibre members balancing prominent expertise from the higher education, research, business and innovation fields. The Governing Board consists of a chairman, a vice-chairman, four executive members, together forming the executive committee. Another thirteen members complete the Governing Board. Chairman of the Board is Dr. Martin Schuurmans, from the Netherlands. He is the former Executive Vice President, Philips Research / Philips Medical systems (PMS). The EIT will be set up following an incremental growth path. An initial contribution from the EU budget (Euro 308.7 million) will help to launch the EIT and the KICs during the 2009-2013 periods and will provide the support structure and the conditions necessary for knowledge transfer and networking. KICs will draw on a variety of sources in order to ensure a sound financial base: • national/regional funding – e.g. grants from national educational or research councils; • community (non-EIT) funding - e.g. FP7 research grant or structural funding; • private funding – e.g. grant from a private foundation or contribution from private business; • the participant's own resources - e.g. cash from the participant's own treasury or in-kind contributions such as the use of buildings (teaching facilities, laboratories, offices) or staff that the partners place at the disposal of the KIC without charge; • EIT funding – the EIT grant to the KIC The EU contribution will act as leverage. The EIT annual grant will be allocated to the KICs on a competitive basis and may be used to fund KIC added value actions within the KIC program up to 100%. KIC added value actions are the activities that 'make a KIC a KIC' and, for example, may include: • the establishment, administration and coordination of the KIC; • provision of EIT branded master, doctorate and post doctorate programmes within a KIC; • mobility schemes within the KIC; • KIC specific IP activities; • incubation of KIC start-ups and spin-offs; Through their strong business component, the KICs will become increasingly attractive targets for investment from the private sector. As the initiative is likely to generate considerable returns, businesses will be expected to lead the way in unleashing Europe's innovation potential by buying into and shaping the KICs with human and financial resources. Private sector investment in the EIT should be completed by philanthropic contributions such as donations or bequests: in order to facilitate the generation of financial resources, the EIT will establish the EIT Foundation with the objective of promoting and supporting its activities.

Name	**ENISA – European Network and Information Security Agency**
Link	http://www.enisa.europa.eu
Structure	The purpose of ENISA is ensuring a high and effective level of network and information security within the Community and develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market. The Agency shall assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security.

	• The Management Board of ENISA is composed of representatives of the Member States, the Commission and of the Stakeholders. • The Permanent Stakeholders' Group (PSG) is composed of 30 high-level experts from all over Europe. They are drawn from relevant stakeholder groups such as the information and communication technologies (ICT) industry, ICT user organisations and academic experts in network and information security. • National Liaison Officers network: Member States representatives - one from each EU and EEA country - are part of the NLO network. A representative from the European Commission and a representative from the Council of the European Union are also part of the network. Although not formally based on the ENISA Regulation, NLOs serve as ENISA's important point of reference into the Member States on specific issues.
Mission, goals and objectives	• The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems. • The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in its Regulation. • Building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors. • The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security. ENISA shall perform the following tasks: • collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission; • provide the European Parliament, the Commission, European bodies or competent national bodies appointed by the Member States with advice, and when called upon, with assistance within its objectives; • enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies; • facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues; • contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of

	alerting users, and seeking synergy between public and private sector initiatives; • assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products; • track the development of standards for products and services on network and information security; • advise the Commission on research in the area of network and information security as well as on the effective use of risk prevention technologies; • promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations; • contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security; • express independently its own conclusions, orientations and give advice on matters within its scope and objectives.

Additional information	ENISA has organised the following activities:
	• Secure Applications and Services: The Secure Applications and Services (SAS) group at ENISA addresses the security of services and applications, ranging from cloud-based services, web applications to smartphones and smartphone apps. ENISA does this by giving stakeholders (EU businesses, government organisations, consumers and consumer organisations) an overview of relevant information security risks and by making risk-based recommendations: publishing guidelines, best practices, and information security governance tools.
	• CERT (Computer Emergency Response Team): Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more. They must act as primary security service providers for government and citizens. At the same time, they must act as awareness raisers and educators. Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISA's mission to, as much as we can, clear out the "white spots" on the CERT world map and to minimise the gaps by facilitating setting-up, training and exercising of CERTs.
	• Identity, Privacy and Trust: Identity, Privacy and Trust are the parallel lanes of the road towards communication networks that safeguard the EU society. As society becomes increasingly dependent on information and communication technologies, Identity, Privacy and Trust are the parallel lanes of the road towards communication networks that safeguard the EU society. The Declaration of the Future Internet Assembly (FIA) "Towards a European approach to the Future Internet" envisages the development and deployment of technologies ensuring the robustness and security of the networks, managing identities, protecting privacy and creating trust in the on-line world. ENISA is approaching this area with the following strategy:
	  • Facilitating rapid deployment of research results: focusing on alternative trust models such as reputation and web-of trust, as well as a stock-taking of authentication methods;
	  • Fostering a Pan-European approach to privacy: focusing on rights and obligations of users as well as service-providers. Providing guidelines on the use of available privacy enhancing technologies and their implications for anonymity;
	  • Development of guidelines for regulatory review and interpretation: focusing

on identity and authentication in new scenarios (e.g. RFID, cloud computing). To avoid unrealistic requirements on commercial bodies and infringement of personal liberties.

- Resilience of public Communication Networks and Services: Reliable communications networks and services are now critical to public welfare and economic stability. Attacks on Internet, disruptions due to physical phenomena, software and hardware failures, and human mistakes all affect the proper functioning of public eCommunications networks. Such disruptions reveal the increased dependency of our society to these networks and their services. The experience has revealed that any country, acting independently, may face difficulties in effectively preventing and responding to this type of attacks which often originate from beyond national and European borders. European Commission's Communications highlight the importance of network and information security and resilience. They stressed the importance of dialogue, partnership and empowerment of all stakeholders to properly address these threats and especially citizen's confidence in infrastructures. EU Commission's recent Communication on CIIP recognises the importance of the area and confirms ENISA's role and expertise in the field. ENISA, fully recognizing this need, devised a Multi-annual Thematic Program (MTP) with the ultimate objective to collectively evaluate and improve the resiliency of public eCommunication Network and Services in Europe. To achieve this objective, ENISA organised its work in three different but complementary areas of interest:
  - The Policy and Strategy area deals with the national policies and regulatory environments across the EU Member States
  - The Providers area focuses on practices, norms, procedures and techniques adopted by providers to enhance the resilience of their networks
  - The Technology area analyses related technologies and highlights their security and resilience aspects (e.g. DNSSec, MPLS, BGP).
- Risk Management: The present ENISA site is the central hub of information about Risk Management / Risk Assessment developed and maintained by ENISA. This site encompasses a variety of information pertinent to Risk Management and Risk Assessment but it also gives information about activities and events in that area. Target group of this content are all kinds of users (e.g. experts and non experts) who are interested to learn more about Risk Management, to get informed about current development and trends in that area or to apply existing Risk Management practices to their organisation. Numerous issues in the area of Risk Management addressed through the ENISA work Programmes will be gradually integrated into this site, such as:
  - Inventories of methods tools and good practices
  - Achieved results in the area of Emerging Risks
  - Information material for Small and Medium Enterprises (SMEs)
  - Comparability and interoperability issues of methods, tools and good practices
  - Integration issues of Risk Management with other operational processes

All this information will be published both by means of interlinked content and downloadable reports. Besides this kind of information, ENISA will inform interested users about relevant events in this field, about the activities of the ENISA ad hoc Working Group on Risk Management / Risk Assessment, about relevant national and international sources of information, etc. In the middle term, ENISA intents to develop this site to a significant collection of knowledge in the area of Risk Management / Risk Assessment for all interested European stakeholders.

- Stakeholder Relations: ENISA's stakeholder relations are a key factor in the success of its overall mission of contributing to the security of the EU internal market. The Management Board (composed of the Commission, Member State and private sector representatives) and Permanent Stakeholder Group (composed of multi-stakeholders), as well as ENISA's informal networks and expert working parties, give us unparalleled insights and access to public and private sector Network and Information Security (NIS) experts. This in turn enables us to identify emerging risks, to forge new insights into help Member States and private sector organisations better prepare themselves for challenges in a proactive and increasingly professional manner, and to build novel public and private sector partnerships as necessary. Activities and deliverables:
  - Managing networks of EU, sectoral, national and international stakeholders

	• Thematic reports • Good practice brokerage • Country reports • ENISA Quarterly Review.

C.2. Regulators

Name	**ACER Cooperation of Energy Regulators**
Link	http://www.energy-regulator.eu/portal/page/portal/ACER_HOME
Structure	The Agency for the Cooperation of Energy Regulators was established by Regulation (EC) No 713/2009 of 13 July 2009. The Third Legislative Package for the Liberalisation of the Energy Market establishes an Agency for the Cooperation of Energy Regulators (ACER). The Regulation establishing ACER ((EC) No 713/2009) is part of a set of five legislative acts adopted in summer 2009 aimed at improving the functioning of Europe's electricity and gas markets. ACER is made up of a) a Board of Regulators comprising a senior representative and one alternate of the EU Member States' 27 national regulatory authorities (NRAs) and one non-voting Commission representative; b) an Administrative Board comprising 9 members and one alternate for each, of which 2 members (and their alternates) are appointed by the European Commission, 2 (and their alternates) by the European Parliament and 5 (and their alternates) by the Council; c) a Director; and d) a Board of Appeal.
Mission, goals and objectives	ACER will play a key role in the liberalisation of the Community electricity and natural gas markets. ACER will at EU-level complement and coordinate the work of the NRAs. Its competences will include participation in the creation of European network rules; taking binding individual decisions on terms and conditions for access and operational security for cross border infrastructure if NRAs cannot agree; giving advice on various energy-related issues to the European institutions; and monitoring and reporting to the European Parliament and the Council. ACER's mission is to assist National Regulatory Authorities in exercising, at Community level, the regulatory tasks that they perform in the Member States and, where necessary, to coordinate their action. The Agency for the Cooperation of Energy Regulators (ACER) is a European Union body established in 2010 and has its official seat in Ljubljana, Republic of Slovenia.
Additional information	ACER will complement and coordinate the work of National Regulatory Authorities (NRAs). Its competences will include participation in the creation of European network rules; taking binding individual decisions on terms and conditions for access and operational security for cross border infrastructure if NRAs cannot agree; giving advice on various energy related issues to the European institutions; and monitoring and reporting to the European Parliament and the Council. ACER will have an Administrative Board, a Regulatory Board and a Board of Appeal. A Director, who is appointed by the Administrative Board after a favourable opinion from the Regulatory Board, will represent the Agency. It is expected that the Agency will have a staff of around 50 people. Its budget will be in the order of EUR 5 million per year. ACER will initially be located in Brussels, Belgium. As of 3 March 2011, ACER will be fully operational in its permanent office in Ljubljana, Slovenia.

Name	**CEER**
Link	http://www.energy-regulators.eu/portal/page/portal/EER_HOME
Structure	CEER is the 'Council of European Energy Regulators'. It is a 'not-for-profit association' under Belgian law and has a Brussels-based Secretariat. In March 2000, ten national energy regulatory authorities signed the 'Memorandum of Understanding for the establishment of the Council of European Energy Regulators'. They had voluntarily formed the council to facilitate cooperation in their common interests for the promotion of the internal electricity and gas market. In order to cope with a growing number of issues and to improve cooperation at the operational level, the regulators decided in 2003 to formally establish themselves as a not-for-profit association under Belgian law and to set up a small secretariat in Brussels. The Statutes (English version, Statutes amendment) were published in the annex of the Belgian State Gazette on October 21st, 2003. The CEER now has 29 members - the energy regulators from the 27 EU-Member States plus Iceland and Norway.

Mission, goals and objectives	The overall aim of the Council of European Energy Regulators (CEER) is to facilitate the creation of a single, competitive, efficient and sustainable internal market for gas and electricity in Europe. The CEER acts as a platform for cooperation, information exchange and assistance between national energy regulators and is their interface at European level with the European Commission, in particular the Directorate General Transport and Energy (DG ENER), DG Competition and DG Research. It cooperates with the European Commission and competition authorities in order to ensure consistent application of competition law to the energy industry. CEER also strives to share regulatory experience worldwide through its links with similar associations in America (NARUC) and in Central/Eastern Europe (ERRA) and its membership in the International Confederation of Energy Regulators (ICER). CEER has taken a central role in developing an effective and competitive electricity and gas market in the Energy Community of South East Europe.
Additional information	-

Name	**ERGEG, the European Regulators' Group for Electricity and Gas**
Link	http://www.energy-regulators.eu/portal/page/portal/EER_HOME
Structure	ERGEG was set up by the European Commission (Decision of November 11, 2003 2003/796/EC) as its advisory body on internal energy market issues. It is made up of the national energy regulatory authorities of the EU's Member States. Its purpose is to facilitate a consistent application, in all Member States, of the provisions set out in Directive 2003/54/EC, Directive 2003/55/EC and Regulation (EC) No 1228/2003, as well as of possible future Community legislation in the field of electricity and gas'.
Mission, goals and objectives	ERGEG advises and assists the Commission on its own initiative or upon request, in particular with respect to the preparation of draft implementing measures in the field of electricity and gas. For example, ERGEG provided significant input to the European Commission in the preparation of its third energy liberalisation legislative package (adopted in September 2007). One of ERGEG's flagship projects is the Regional Initiatives, which it launched with the Commission's backing in Spring 2006, in an effort to speed up the integration of Europe's national energy markets. The ERGEG Regional Initiatives establish 7 electricity and 3 regional gas markets in Europe as an intermediate step to the creation of a single, competitive EU market in electricity and gas.
Additional information	The Regional Initiatives is the regulators' flagship project to speed up the integration of Europe's national energy markets. The Regional Initiatives has created 3 regional markets for gas and 7 for electricity in Europe. ERGEG and the European Commission work at EU level to ensure the coherence and convergence of these regions towards the ultimate goal, a single-EU energy market.

C.3. Branch organisations

Name	**EDSO FOR SMART GRIDS AISBL (European Distribution System Operators)**
Link	https://www.edsoforsmartgrids.eu/
Structure	EDSO for Smart Grids is a non-profit organisation founded in March 2010 in Belgium, to structure, lead and enhance, non-profit cooperation between European Distribution System Operators for electricity as well as to assure, manage, represent and promote their common interests, specifically on Smart Grids development and implementation. EDSO for Smart Grids Association represents 27 leading actors in 16 countries of the European Union reaching more than 70% of its electricity metering points. EDSO for Smart Grids is one of the three industry partners along with the European Technology Platform for Smart Grids and ENTSO-E invited by the SET-Plan Secretariat of the European Commission to constitute (together with Member States and European Commission) the Electricity Grid EII (European Industrial Initiative) launched in Madrid on June 3rd and 4th 2010.
Mission, goals and objectives	The goal of EDSO for Smart Grids is promoting the development of Smart Grids in Europe so to ensure the reliability of the electricity distribution grids, as well as their optimal management and technical

	development, to reach the European energy goals of security of supply, sustainability and market efficiency. In this regards the European Electricity Grid Initiative aims to develop, demonstrate and validate, at scale, the technologies needed to: • Enable the transmission and distribution of up to 35 % of electricity from dispersed and concentrated renewable energy sources by 2020 and make electricity production completely decarbonised by 2050. • Further integrate national networks into a truly pan-European, market based network. • Optimise the investments and operational costs involved in upgrading the European electricity networks to respond to the new challenges. • Guarantee a high quality of electricity supply to all customers and engage them as active. EDSO for Smart Grids aims also to play an important and active role in the future European regulatory process (in accordance with community legislation), regarding the Smart Grids development and implementation.
Additional information	EDSO for Smart Grids can carry out all necessary activities to achieve, directly or indirectly, the objectives and common interests of its Members by: • PROMOTING: The development of an efficient, secure and sustainable distribution grid; the standardisation, the interoperability and flexibility of equipment and solutions; the preparation and management of research, development and demonstration activities. • MANAGING: Technical information and best practice sharing among its members and other electricity stakeholders; funding mechanisms. • STUDYING: The regulatory principles and organizing seminars or conferences in order to communicate the results of its working groups.

Name	**ENTSO-E (European Network of Transmission System Operators for Electricity)**
Link	https://www.entsoe.eu/
Structure	ENTSO-E is the European Network of Transmission System Operators for Electricity, representing 42 Transmission System Operators (TSOs) from 34 countries. Founded in December 2008, it's legal raison d'être is Regulation (EC) 714/2009 on electricity cross-border exchanges. EDSO-Smart Grid (European DSO Association for Smart Grids) has recently been created by a number of Distribution System Operators and is open to wide membership. The two associations, jointly with the European Technology Platform Smart Grids will play an important role in the planning, monitoring and dissemination of this initiative. In the dissemination of the results regarding the distribution network, Eurelectric will also play a key role.
Mission, goal and objectives	Being the body of transmission system operators of electricity at European level, ENTSO-E's mission is to promote important aspects of energy policy in the face of significant challenges: • Security - it pursues coordinated, reliable and secure operations of the electricity transmission network. • Adequacy - it promotes the development of the interconnected European grid and investments for a sustainable power system. • Market - it offers a platform for the market by proposing and implementing standardised market integration and transparency frameworks that facilitate competitive and truly integrated continental-scale wholesale and retail markets. • Sustainability - it facilitates secure integration of new generation sources, particularly growing amounts of renewable energy and thus the achievement of the EU's greenhouse gases reduction goals. The activities are focused on:

	• Reliable operation • Optimal management • Sound technical evolution of the European electricity grid • Security of supply • Meeting the needs of the Internal Energy Market and facilitating market integration • Network development statements • Network codes • Promotion of relevant R&D and the public acceptability of transmission infrastructure Consultation with stakeholders and positions towards energy policy issues.
Additional information	The European Network of Transmission System Operators for Electricity speaks for all electric TSOs in the EU and others connected to their networks, with one voice for all regions, and for all their technical and market issues. Transmission System Operators (TSOs) are responsible for the bulk transmission of electric power on the main high voltage electric networks. TSOs provide grid access to the electricity market players (i.e. generating companies, traders, suppliers, distributors and directly connected customers) according to non-discriminatory and transparent rules. In order to ensure the security of supply, they also guarantee the safe operation and maintenance of the system. In many countries, TSOs are in charge of the development of the grid infrastructure too. TSOs in the European Union internal electricity market are entities operating independently from the other electricity market players. In ENTSO-E the TSOs cooperate regionally and on the European scale, and through ENTSO-E they communicate their needs and positions on European and regional issues. ENTSO-E's activities are organised in the three Committees along which the website is structured, for System Development, System Operations and Market, and are supported by a Legal & Regulatory Group. ENTSO-E's vision is to become and remain the focal point for all European, technical, market and policy issues related to TSOs, interfacing with the power system users, EU institutions, regulators and national governments. ENTSO-E's work products contribute to security of supply, a seamless, pan-European electricity market, a secure integration of renewable resources and a reliable future-oriented grid, adequate to energy policy goals.

Name	**EURELECTRIC The Union of the Electricity Industry**
Link	http://www.eurelectric.org/
Structure	EURELECTRIC's Full Member structure is based on national representation, via the national electricity association, where such a body exists, or the leading electricity enterprise in each country. Currently there are 33 Full Members, including all 27 EU Member States, current applicants negotiating to join the Community, plus other European OECD countries. Full Members, plus observers representing both European and Mediterranean Affiliates, have a seat on the Board of Directors, the supreme governing body, whose main task is to set EURELECTRIC's work agenda and determine its main policies and strategies. EURELECTRIC also currently has 22 non-voting Affiliate Members representing the electricity industry across the rest of Europe, in the Mediterranean basin and on four other continents. Membership is completed by 12 Associate Members drawn from the electricity sector, plus 24 Business Associates from other sectors with stakeholder links to or interest in the electricity industry. The EURELECTRIC President is elected for a period of three years and is supported by a Vice-President, also with a mandate of three years. EURELECTRIC's opinions and policy positions are formulated in some 30 expert Working Groups, supervised by five Committees, each of which adopts positions or undertakes studies on all issues within its competence. This 'structure of expertise' ensures that input to EURELECTRIC positions comes from several hundred active electricity sector professionals and that our Members are profoundly involved in forging common views on subjects of shared interest.
Mission, goals and objectives	EURELECTRIC's mission is to contribute to the development and competitiveness of the electricity industry and to promote the role of electricity in the advancement of society. It pursues in all its activities the application of the following sustainable development values: • Economic Development • Growth, added-value, efficiency • Environmental Leadership • Commitment, innovation, pro-activeness • Social Responsibility • Transparency, ethics, accountability. Currently, EURELECTRIC's three paramount objectives are:

	• supporting the process of market liberalisation in our sector, helping to create a pan-European energy market through harmonisation and industry action; • contributing to the pan-European integration of the electricity industry and to the creation of a fruitful business environment across the continent; • fostering the integration of a sustainable development approach in electricity industry strategies and policies and promoting recognition of electricity as part of the solution to these concerns through market-oriented policies.
Additional information	Within the European Union, EURELECTRIC represents the electricity industry in public affairs, in particular in relation to the EU legislative institutions in order to promote the interests of its Members at a political level.

Name	**CEDEC: The European Federation of Local Energy Companies**
Link	http://www.cedec.com/home_en.aspx?l=en
Structure	Membership of CEDEC is open to all local and regional energy utilities in Europe.
Mission, goals and objectives	The CEDEC mission is to: • represent the interests of the local and regional energy companies in electricity and gas vis-à-vis the European institutions; • exchange experiences and information concerning energy policy and regulation for local and regional energy distribution in Europe; • cooperate in view of (inter)national support.
Additional information	Founded in 1992 and with company seat in Brussels, the European Federation of Local Energy Companies represents the interests of 2000 local utilities in the electricity and gas sector at European level with a total turnover of 100 billion Euros, more than 250.000 employees, and serving 75 million electricity and gas customers & connections. These predominantly medium-sized local and regional energy companies have developed activities as electricity and heat generators, electricity and gas distribution grid & metering operators and energy (services) suppliers.

Name	**EUTC European Utilities Telecom Council**
Link	http://www.eutc.org/
Structure	European Utilities Telecom Council (EUTC) represents the telecommunications and information technology interests of Europe's electric, gas and water utilities and other critical infrastructure organisations.
Mission, goals and objectives	European Utilities Telecom Council's primary purpose is to create a favourable regulatory, technical and business environment in which its members will: • be equipped to provide the most secure, reliable and cost effective core business operational communications networks; • have every opportunity to succeed in the competitive European telecommunications market.
Additional information	Technology is rapidly changing the role of telecom in Europe's electric, gas and water utilities, energy companies and other critical infrastructure companies. Many are using their vast experience in building and managing sophisticated telecommunications networks to enter Europe's new competitive telecoms markets. Many are also facing issues introducing new wireless communications systems and managing internal telecoms businesses in a shared services environment. For decades European Utilities Telecom Council's members have constructed, owned and managed some of Europe's largest private fibre and wireless communications networks used to ensure safe, secure and reliable delivery of essential utility services. Today, European utilities are faced with new regulatory, technological and business challenges to maintain the high quality of these private networks. At the same time, many are actively engaged in using their telecom experience to develop and deliver new, competitive commercial communication services to better serve their communities.

Name	**GEODE: is the European Association of distribution energy companies both of electricity and gas**

Link	http://www.geode-eu.org
Structure	GEODE membership is open to all companies with an interest in the distribution of energy in Europe.
Mission, goals and objectives	GEODE represents the interests of the independent European distributors in front of European energy authorities and allows the exchange of expertise among their members. GEODE believes in the liberalisation of the energy market and supports the achievement of a single European integrated market.
Additional information	Founded in 1991, GEODE represents more than 600 independent distribution companies of gas and electricity, both private and publicly owned, located in eleven European countries as Austria, Bulgaria, Denmark, Germany, Hungary, Italy, Norway, Slovenia, Spain, Sweden, and UK.

C.4. Research and standardisation bodies

C.4.1. EU Standardisation

Name	**CEN - European Committee for Standardisation**
Link	http://www.cen.eu
Structure	CEN's 31 National Members work together to develop voluntary European Standards (ENs). ENs help build a European Internal Market for goods and services and position Europe in the global economy. More than 60.000 technical experts as well as business federations, consumer and other societal interest organisations are involved in the CEN network that reaches over 480 million people.
Mission, goals and objectives	The European Committee for Standardisation (CEN) is a business facilitator in Europe, removing trade barriers for European industry and consumers. Its mission is to foster the European economy in global trading, the welfare of European citizens and the environment. Through its services it provides a platform for the development of European Standards and other technical specifications. These standards have a unique status since they also are national standards in each of its 31 Member countries. With one common standard in all these countries and every conflicting national standard withdrawn, a product can reach a far wider market with much lower development and testing costs. CEN is a major provider of European Standards and technical specifications. It is the only recognised European organisation according to Directive 98/34/EC for the planning, drafting and adoption of European Standards in all areas of economic activity with the exception of electro-technology (CENELEC) and telecommunication (ETSI).
Additional information	In a globalised world, the need for international standards simply makes sense. The Vienna Agreement – signed by CEN in 1991 with ISO (International Organisation for Standardisation), its international counterpart – ensures technical cooperation by correspondence, mutual representation at meetings and coordination meetings, and adoption of the same text, as both an ISO Standard and a European Standard.

Name	**CENELEC, the European Committee for Electro-technical Standardisation**
Link	http://www.cenelec.eu
Structure	CENELEC, the European Committee for Electro-technical Standardisation, was created in 1973 as a result of the merger of two previous European organisations: CENELCOM and CENEL. Nowadays, CENELEC is a non-profit technical organisation set up under Belgian law and composed of the National Electro-technical Committees of 31 European countries. In addition, 11 National Committees from neighbouring countries are participating in CENELEC work with an Affiliate status. CENELEC members have been working together in the interests of European harmonisation since the 1950s, creating both standards requested by the market and harmonised standards in support of European legislation and which have helped to shape the European Internal Market. CENELEC works with 15,000 technical experts from 31 European countries. Its work directly increases market potential, encourages technological development and guarantees the safety and health of consumers and workers.
Mission, goals and objectives	CENELEC's mission is to prepare voluntary electro-technical standards that help develop the Single European Market/European Economic Area for electrical and electronic goods and services removing barriers to trade, creating new markets and cutting compliance costs.
Additional information	A Resolution of 7th May 1985 of the European Council formally endorsed the principle of reference to European standards within the relevant European regulatory work (Directives), thereby paving the way to a New Approach in the philosophy of regulations and standards in Europe. In the light of this New Approach, CENELEC is developing and achieving a coherent set of voluntary electro-technical standards

	as a basis for the creation of the Single European Market/European Economic Area without internal frontiers for goods and services. In addition to the traditional European standard deliverables, the dynamic Workshop (CWA: CENELEC Workshop Agreement) has been included in its portfolio, offering an open platform to foster the development of pre-standards for short lifetime products where time-to-market is critical.

Name	**ETSI - European Telecommunications Standards Institute**
Link	http://www.etsi.org
Structure	ETSI is a not-for-profit organisation with more than 700 ETSI member organisations drawn from 62 countries across 5 continents world-wide. ETSI's purpose is to produce and perform the maintenance of the technical standards and other deliverables which are required by its members (Article 2 of the ETSI Statutes - see ETSI Directives). Like most standards organisations, much of this work is carried out in committees and working groups composed of technical experts from the Institute's member companies and organisations. These committees are often referred to as 'Technical Bodies' (TB), and typically meet between two and six times a year, in the ETSI premises or elsewhere. They also rely heavily on electronic communications to help progress the work, especially in-between meetings. For certain urgent items of work, where this frequency of meeting is not sufficient, ETSI may also convene a Specialist Task Force (STF). STFs are small groups of technical experts usually seconded from ETSI members, to work intensively over a period of time, typically a few months, to accelerate the drafting work. Each STF reports to an ETSI technical body. In addition, ETSI provides a number of other services related to standardisation, such as interoperability events (Plugtests™), testing and interoperability related services and hosting. The work of ETSI, including that of its Technical Bodies and Specialist Task Forces, is governed by the ETSI Directives, a set of documents that define the legal status, purpose, scope, and functional aspects of the Institute. These Directives cover the entire lifecycle of ETSI's standards and other products, from inception, through drafting and approval, to publication, and then subsequent maintenance and finally, where necessary, withdrawal from public availability. Maintenance of the ETSI Directives is the responsibility of the General Assembly, supported by the ETSI Board. ETSI recognises three types of Technical Body: • Technical Committee: a Technical Committee is a semi-permanent entity organised around a number of standardisation activities addressing a specific technology area. The results of a Technical Committee's work may often be used by other Technical Committees. • ETSI Project: an ETSI Project is similar to a Technical Committee but is established on the basis of a market sector requirement rather than on a basic technology, is therefore more self-contained, and has a defined duration. • ETSI Partnership Project: an ETSI Partnership Project is an activity established when there is a need to co-operate with other organisations to achieve a standardisation goal and where that co-operation cannot be accommodated within an ETSI Project or Technical Committee. • Each may establish Working Groups if required. The Chairman of a Technical Body is nominated by the committee and is appointed by the ETSI Board. He or she is responsible for the overall management of the committee, its working groups and its work program. Representatives of Full and Associate Members have the right to participate in the work of a technical body and its working groups. Others may participate only under exceptional circumstances. Working documents are usually available only to members of ETSI, but the technical body's output of standards and reports, once approved, are made available in the public domain, free of charge. The technical bodies are overseen by an Operational Co-ordination Group (OCG), comprising the technical bodies Chairmen, but they are ultimately accountable to the ETSI Board and General Assembly. The ETSI Secretariat provides a range of support services to the technical bodies. Industry Specification Groups exist alongside the current Technical Organisation supplementing the existing standards development process. An Industry Specification Group, supported by Working Groups where appropriate, is an activity organised around a set of ETSI work items addressing a specific technology area.
Mission, goals and objectives	The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.
Additional information	ETSI is officially recognised by the European Union as a European Standards Organisation. The high quality of their work and open approach to standardisation has helped evolve into a European roots global branches operation with a solid reputation for technical excellence.

	Each technical body establishes and maintains a work program, consisting of Work Items. An ETSI Work Item is the description of a standardisation task, and normally results in a single standard, report, or similar document. The technical body approves each Work Item, which is then formally adopted by the whole membership (via a web-based procedure). Collectively, the work programs of all the technical bodies constitute the ETSI Work Program. A technical body usually gives responsibility for a Work Item to a small group of experts, led by a Reporter. The document (standard, report etc.) resulting from the Work Item is referred to as an ETSI Deliverable, which may be an: • ETSI Technical Specification (TS) • ETSI Technical Report (TR) • ETSI Standard (ES) • ETSI Guide (EG) • European Standard (or European Norm, EN) • ETSI Special Report (SR) • ETSI Group Specification (GS) The ability to produce these different types of documents allows ETSI to respond a variety of needs within the industries it serves. Very occasionally, the Work Item may not lead to any of the above types of deliverable, in which case it is called a Miscellaneous Item. The Reporter Groups, Working Groups, and the technical committee as a whole carry out their work by electronic means, including e-mail, e-mail exploders and the ETSI server, as well as in physical meetings. The use of the electronic methods, both within and apart from physical meetings, has been found to dramatically increase the speed and efficiency of standards-making. A technical body takes its decisions, including approval of draft Deliverables, either by simple consensus or by a weighted vote. Each Member company or organisation has a voting weight determined by its membership fee, which in turn depends upon the company's financial turnover and other factors. A proposition passes if at least 71% of the weighed votes cast are in favour. In the case of ETSI Technical Specifications and ETSI Technical Reports, the technical body approves the Deliverable for publication. For other Deliverables, the technical body approves the Work Item result, which is then submitted to further levels of approval before publication: these depend on the type of Deliverable. ETSI provides web-based applications to assist the voting process and the determination of the result. An Industry Specification Group (ISmart Grid) may establish its own procedures for the creation and approval of Group Specifications, within the broad framework of the ETSI Directives. ETSI M2M is the technical committee coordinating ETSI involvement in the Smart Metering (M/441) and Smart Grids (M/490) standardization mandates, accepted jointly with CEN and CENELEC. This participation incorporates the mandates-related activities of several other ETSI TCs, namely TC PLT, ERM, ATTM, SCP, MSG and TISPAN. . The communication architecture proposed in the smart metering standardisation work coordinated by ETSI/CEN/CENELEC deviates from the ETSI M2M communication architecture proposal in that sense that ETSI M2M proposes an end-to-end full IPv6 communication platform, while the other group builds on the current day solutions.

C.4.2. Worldwide standardisation

Name	**NIST – National Institute of Standards and Technology**
Link	http://www.nist.gov
Structure	Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Mission, goals and objectives	NIST carries out its mission in four cooperative programs: the NIST Laboratories, conducting research that advances the nation's technology infrastructure and is needed by U.S. industry to continually improve products and services; • the Baldrige Performance Excellence Program, which promotes performance excellence among U.S. manufacturers, service companies, educational institutions, health care providers, and nonprofit organisations; conducts outreach programs and manages the annual Malcolm Baldrige National Quality Award which recognizes performance excellence and quality achievement; • the Hollings Manufacturing Extension Partnership, a nationwide network of local centers offering technical and business assistance to smaller manufacturers; and • the Technology Innovation Program, which provides cost-shared awards to industry, universities, and consortia for research on potentially revolutionary technologies that address critical national and societal needs.

	• Between 1990 and 2007, NIST also managed the Advanced Technology Program.
Additional information	NIST's FY 2010 resources total $856.6 million from the Consolidated Appropriations Act of 2010 (Public Law 111-117), $49.9 million in service fees, and $101.5 million from other agencies. The agency operates in two locations: Gaithersburg, Md., (headquarters—234-hectare/578-acre campus) and Boulder, Colo., (84-hectare/208-acre campus). NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. Also, NIST hosts about 2,600 associates and facility users from academia, industry, and other government agencies. In addition, NIST partners with 1,600 manufacturing specialists and staff at about 400 MEP service locations around the country.

Name	**IEEE - Institute of Electrical and Electronic Engineers**
Link	http://www.ieee.org
Structure	The IEEE-SA is governed by the Board of Governors (BOG) who are elected by IEEE-SA Members. The Board of Governors oversees number of committees that are dedicated to manage key operational aspects of the IEEE-SA. The IEEE-SA Standards Board reports directly to the BOG, and oversees the IEEE standards development process. Standards Board members are elected by IEEE-SA members as a privilege of membership, and all Board Members and Committee members must be IEEE-SA members in good standing.
Mission, goals and objectives	The IEEE Standards Association (IEEE-SA) is a leading consensus building organisation that nurtures, develops and advances global technologies, through IEEE. They bring together a broad range of individuals and organisations from a wide range of technical and geographic points of origin to facilitate standards development and standards related collaboration. With collaborative thought leaders in more than 160 countries, IEEE promote innovation, enable the creation and expansion of international markets and help protect health and public safety. Collectively, their work drives the functionality, capabilities and interoperability of a wide range of products and services that transform the way people live, work and communicate.
Additional information	The IEEE-SA standards development process is open to IEEE-SA Members and non-members, alike. However, IEEE-SA Membership enables standards development participants to engage in the standards development process at a deeper and more meaningful level, by providing additional balloting and participation opportunities. IEEE-SA members are the driving force behind the development of standards, providing technical expertise and innovation, driving global participation, and pursuing the ongoing advancement and promotion of new concepts. Among other, the European utilities ERDF and Iberdrola are the driving forces behind the currently developed 1901.2 communication standard for Smart Grids. A full IPv6 communication network platform will be the starting for the development and standardisation of the communication technology.

Name	**IEC - International Electro-technical Commission**
Link	http://www.iec.ch
Structure	Through its members, the IEC promotes international cooperation on all questions of electro-technical standardisation and related matters, such as the assessment of conformity to standards, in the fields of electricity, electronics and related technologies. The IEC charter embraces all electro-technologies including electronics, magnetics and electro-magnetics, electro-acoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electro-magnetic compatibility, measurement and performance, dependability, design and development, safety and the environment.
Mission	The International Electro-technical Commission (IEC) is the leading global organisation that prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardisation and as references when drafting international tenders and contracts.
Objectives	The IEC objectives are to: • Meet the requirements of the global market efficiently • Ensure primacy and maximum world-wide use of its standards and conformity assessment systems • Assess and improve the quality of products and services covered by its standards • Establish the conditions for the interoperability of complex systems • Increase the efficiency of industrial processes • Contribute to the improvement of human health and safety

	• Contribute to the protection of the environment.
Additional information	IEC's international standards facilitate world trade by removing technical barriers to trade, leading to new markets and economic growth. Put simply, a component or system manufactured to IEC standards and manufactured in country A can be sold and used in countries B through to Z. IEC's standards are vital since they also represent the core of the World Trade Organisation's Agreement on Technical Barriers to Trade (TBT), whose 100-plus central government members explicitly recognise that international standards play a critical role in improving industrial efficiency and developing world trade. The number of standardisation bodies which have accepted the Code of Good Practice for the Preparation, Adoption and Application of Standards to the WTO's TBT Agreement underlines the global importance and reach of this accord. IEC standards provide industry and users with the framework for economies of design, greater product and service quality, more inter-operability, and better production and delivery efficiency. At the same time, IEC's standards also encourage an improved quality of life by contributing to safety, human health and the protection of the environment. The IEC's multilateral conformity assessment systems, based on its international standards, are truly global in concept and practice, reducing trade barriers caused by different certification criteria in various countries and helping industry to open up new markets. Removing the significant delays and costs of multiple testing and approval allows industry to be faster and cheaper to market with its products. As technology becomes more complex, users and consumers are becoming more aware of their dependence on products whose design and construction they may not understand. In this situation, reassurance is needed that the product is reliable and will meet expectations in terms of performance, safety, durability and other criteria. How can the industrial user and the final consumer be sure that the product they buy conforms to the criteria of an IEC standard? The IEC's conformity assessment and product certification systems exist to provide just this reassurance, and the regulatory nature of some products now also sees recognition of the CA systems amongst some government regulators.

Name	**ISO - International Organisation for Standardisation**
Link	www.iso.org
Structure	ISO (International Organisation for Standardisation) is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 163 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.
Mission, goals and objectives	ISO is a non-governmental organisation that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.
Additional information	-

Name	**ITU - International Telecommunication Union**
Link	http://www.itu.int
Structure	ITU is the leading United Nations agency for information and communication technology issues, and the global focal point for governments and the private sector in developing networks and services. For 145 years, ITU has coordinated the shared global use of the radio spectrum, promoted international cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world, established the worldwide standards that foster seamless interconnection of a vast range of communications systems and addressed the global challenges of our times, such as mitigating climate change and strengthening cyber security. ITU is based in Geneva, Switzerland, and its membership includes 192 Member States and more than 700 Sector Members and Associates.
Mission, goals and objectives	From broadband internet to latest-generation wireless technologies, from aeronautical and maritime navigation to radio astronomy and satellite-based meteorology, from convergence in fixed-mobile phone, internet access, data, voice and TV broadcasting to next-generation networks, ITU is committed to connecting the world.

Additional information	ITU also organizes worldwide and regional exhibitions and forums, such as ITU TELECOM WORLD, bringing together the most influential representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology for the benefit of the global community, and in particular the developing world.

Name	**Information Security Forum (ISF)**
Link	http://www.securityforum.org
Structure	Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit organisation that supplies authoritative opinion and guidance on all aspects of information security. By harnessing a combination of our world-renowned in-house expertise and the collective knowledge and experience of our 300 Members around the globe, the ISF delivers practical solutions to overcome wide-ranging security challenges impacting business information today. The ISF is owned by its Members and operated on a day-to-day basis by proven service providers. The ISF is a democratic body, governed by an elected Council and Executive of Members.
Mission, goals and objectives	It may not always be possible for one organisation to build the level of knowledge and expertise needed to keep abreast of diverse information security issues, understand emerging risks and develop good practice solutions. That's why our Members, including many of the world's major corporations (from all sectors), public sector bodies and government departments have joined the ISF. For organisations with a complex set of security requirements, the ISF plays a major role in driving down risk and winning the fight against threats to their information security.
Additional information	-

Name	**ZigBee Alliance**
Link	http://www.zigbee.org
Structure	Established in 2002,the Alliance is an open, non-profit association of members that has created a thriving global ecosystem. Anyone can join the membership comprised of businesses, universities and government agencies from around the globe. The activities and direction are determined by members as they act to meet evolving needs in a fast-paced world.
Mission, goals and objectives	Leveraging our global perspective, we work together to develop standards that ultimately deliver greater freedom and flexibility for a smarter, more sustainable world. As a result of this focus, ZigBee: • Provides green, low-power and open global wireless networking standards focused on monitoring, control and sensor applications. • Allows products to run on harvested energy or batteries for years with its low-power wireless standards, making greener lifestyles possible. • Uniquely connects dramatically different types of devices into a single network, giving you unprecedented control. • Offers a variety of intelligent features designed to ensure devices communicate in any environment, and around the world. • Is simple to set up and can easily grow to meet your needs and deliver years of maintenance-free use.
Additional information	-

D. Relevant legal and framework instruments

402 This is a non exhaustive list of legal inputs and instruments considered for this report at the time of publication:

- European Convention on Human Rights ECHR Art. 8;
- Charter of Fundamental Rights of the European Union CFREU;
- Art. 7: respect for private and family life;
- Art. 8 – Protection of personal data;
- Art. 51(1) – Field of application;
- Art. 52(1) – Scope and interpretation of rights and principles;
- Treaty on the Functioning of the European Union (TFEU) – Art. 16 (ex Art. 286);
- Treaty on the European Union (TEU) – Art. 6 and Art. 39;
- 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 (see also Appendix B);
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services;
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws;
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC;
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC (November 25, 2009);
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters;
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
- Directive 2004/22/EC on measuring instruments (MID);

- Standardisation Mandate M/374 of 20th October 2005 as base for developing standards for utility meters;
- Directive 2006/32/EC on energy end-use efficiency and energy services (Article 13);
- Directives 2009/72/EC and 2009/73/EC ('Third Energy Package');
- Standardisation Mandate M/441 of 12th March 2009 on development of an open architecture for utility meters;
- Standardisation Mandate M/468 of 29th June 2010 concerning the charging of Electric vehicles;
- Directive on a Community framework for electronic signatures (1999/93/EC December 13, 1999).

E. References

1. **The European Union.** *Charter of Fundamental Rights of the European Union 2000/C 364/01*. s.l. : Official Journal of the European Communities, 2000.

2. **Council of Europe.** Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows. [Online] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=13/12/2010&CL=ENG.

3. *The Right to Privacy*. **Brandeis, S.D. Warren and L.D.** 1890, Harvard Law Review, p. Vol.4 No.5.

4. **OECD.** Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [Online] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

5. **Council of Europe.** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. [Online] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=13/12/2010&CL=ENG.

6. **The European Union.** 2007/C 306/01 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. 2007.

7. —. C 11 5/47 The Treaty on the Functioning of the European Union. 2008.

8. —. C 115/13 Treaty on the European Union. 2008.

9. **The European Parliament and the Council.** Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. 24 October 1995.

10. —. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. 12 July 2002.

11. —. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications netwo. 2006.

12. —. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services. 25 November 2009.

13. —. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. 2008.

14. —. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. 2001.

15. —. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications. *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications.* 12 July 2002.

16. **Federation of European Direct and Indirect Marketing.** *European Code of Practice for the Use of Personal Data in Direct Marketing Electronic Communications Annex.* Brussels : s.n., 2010.

17. Expert Group 3: Roles and Responsibilities of Actors involved in the Smart Grids Deployment [Draft]. s.l. : EU Commission Task Force for Smart Grids, December 2010.

18. **The European Parliament and the Council.** *Decision 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC.* 2008.

19. —. Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments. 2004.

20. **Article 29 Data Protection Working Party.** *Opinion 12/2011 on smart metering*. 2011.

21. **Barado, Zeller.** A Face Is Exposed for AOL Searcher No. 4417749. 2006.

22. **Sweeney, L.** Uniqueness of Simple Demographics in the US Population. 2009.

23. **Narayanan, Shmatikov.** How to break anonimity of the Netflix Prize Dataset. 2006.

24. **Council of Europe.** *Data Protection - Compilation of Council of Europe texts.* Strasbourg : Council of Europe, 2010.

25. **CE-RFD (FP7 project).** Privacy and Data Protection Impact Assessment Framework for RFID Applications. 2011 : s.n.

26. **The European Commission.** *A comprehensive approach on personal data protection in the European Union.* 2010.

27. *Understanding the benefits of the Smart Grid.* **DoE National Energy Technology Laboratory.** s.l. : DoE, 2010.

28. **Cyber Security Working Group.** NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements by the The Smart Grid Interoperability Panel. 2010.

29. Expert Group 1: Functionalities of Smart Grids and smart meters. s.l. : EU Commission Task Force for Smart Grids, December 2010.

30. **CEN CENELEC ETSI.** *JWG Report on Standards for Smart Grids* . 2010.

31. **The European Union and the Council.** *Directive 2009/72/EC of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.* 2009.

32. Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003. s.l. : European Parliament and the Council, 13 July 2009.

33. **The European Parliament and the Council.** Directive 2001/77/EC of the European Parliament and of the Council of 27 September 2001 on the promotion of electricity produced from renewable energy sources in the internal electricity market. 2001.

34. —. Directive 2003/30/EC of the European Parliament and of the Council of 8 May 2003 on the promotion of the use of biofuels or other renewable fuels for transport. 2003.

35. —. Directive 2009/28/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing Directives 2001/77/EC and 2003/30/EC. 2009.

36. *Coordinated Control of FACTS Devices in Power Systems for Security Enhancement.* **Gabriela Hug-Glanzmann, Goran Andersson.** 2007, Vol. Bulk power systems dynamics and control.

37. **Ohm, P.** The Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. 2009.

38. **Messick, Graham.** Cyber War: Sabotaging the System. *CBS News.* 8 November 2009.

39. **Luiijff, B. Averill and E.** Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention. *International Journal on Energy Security.* 2010.

40. **Gorman, Siobhan.** Electricity Grid in U.S. Penetrated By Spies . *Wall Street Journal.* 9 April 2009.

41. **Garcia, Jacobs.** Privacy-Friendly Energy-metering via Homomorphic Encryption. 2010.

42. **de Vries K., Bellanova R., De Hert P., Gutwirth S.** The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it?). *Privacy and data protection: an element of choice.*

43. **Danezis, Rial.** Privacy Preserving Metering for Smart Grids (to appear). 2010.

44. **Brickell, Camenisch.** Direct Anonymous Attestation. 2004.

45. **Sean Kelly, Government of South Australia.** Wholesale Pricing in the National Electricity Market. [Online] 4 February 2009. http://www.dtei.sa.gov.au/ECC/media/documents/meeting_85/ECC_pres_040209_Wholesale_Pricing_in_the_NEM.pdf.

46. **Working Party 29.** *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.* 2009.

47. **Damgaard et al.** Secure multiparty computation goes live. 2009.

48. **RIA Novosti.** *Russian nuclear power websites attacked amid accident rumors.* 23 May 2008.

49. **European Commission Directorate-General of Justice.** *Protection of Personal Data in the European Union.* 2010.

50. **Working Party 29.** *Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010.* 2010.

51. *Olsson vs Sweden.* 10465/83, s.l. : ECtHR, 24 March 1988.

52. National provisions communicated by the member states concerning 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 o. [Online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:71995L0046:EN:NOT .

53. **The Council of Europe.** Modernisation of Convention No. 108. [Online] http://www.coe.int/t/dghl/standardsetting/dataprotection/Modernisation_en.asp.

54. **GAO.** Electricity Grid Modernization: Progress being made on cyber security guidelines, but key challenges remain to be addressed. 2011.

55. Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. s.l. : The European Parliamant and the Council, 13 July 2009.

56. **Brattle Group.** *Demand Response, Energy Efficiency, and the Smart Grid.* 2001.

57. **EDPS.** Definition of privacy by the EDPS. [Online] http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Dataprotection/Glossary/pid/84#privacy. .

58. **The White House.** *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* 2009.

59. **The Council of Europe.** *Case Law of the European Court of Human Rights concerning the Protection of Personal Data.* Strasbourg : s.n., 2009.

60. **The European Commission.** A comprehensive approach on personal data protection in the European Union. 2011.

61. **The European Union.** [Online] 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.

62. **Article 29 Working Party.** Opinion 1/2010 on the concepts of "controller" and "processor". 2010.

F. Index

G. Glossary of terms and abbreviations

Term	Meaning
BRP	Balance Responsible Party
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CVR	Conservation Voltage Reduction
DER	Distributed Energy Resources
DG	Distributed Generation
DSO	Distribution System Operator
DSP	Demand Side Participation
DSR	Demand Side Response
EC	European Community
EHV	Extra-high voltage, above 230 kV, ref IEC
EHS	Electromagnetic Hyper-Sensitivity
ELF	Extremely Low Frequency
EMF	Electromagnetic Field
ESO	European Standardisation Organisations
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicles
FAM	Field Area Measurement
FDIR	Fault detection, isolation and restoration
GPRS	General Packet Radio Service
HV	High Voltage, above 35 kV up to and including 230 kV, ref IEC
ICNIRP	International Commission for Non Ionizing Radiation Protection
IEC	International Electrotechnical Commission
ISO	International organisation for Standardisation
ITU-T	International Telecommunication Union
LTE	3GPP Long Term Evolution (LTE), is the latest standard in the mobile network technology
LV	Low Voltage, up to and including 1 kV, ref IEC
MV	Medium Voltage, above 1 kV up to and including 35 kV, ref IEC
MS	Member State
M&D	Monitoring and Diagnostics
PMR	Private Mobile Radio
PMU	Phasor Measurement Unit
PV	Photovoltaic Solar Power
RES	Renewable Energy Sources
SCADA	Supervisory Control and Data Acquisition systems

SCENIHR	Scientific Committee on Emerging and Newly Identified Health Risks
Smart Grid	Smart Grids
SM	Smart Metering
SMCG	Smart Meter Coordination Group (under Mandate 441)
TSO	Transmission System Operator
ToU	Time of Use, the way of pricing of energy depending on the time of its usage
UoS	Use of System
VVO	Volt-Var Optimisation
V2G	Vehicle to Grid
WAM	Wide Area Measurement
WHO	World Health Organisation
Network operators	Transmission (TSO) and distribution system/network operators (DSOs).
Grid users	Generators, customers (including mobile customers), storage owners.
Other actors	Suppliers, metering operators, ESCOs, aggregators, applications and services providers, power exchange platform operators.

H. Questionnaire for DPAs

H.1. DPAs contacted

In the following table the representatives from DPA's in the 27 EU Member States the questions were sent to are listed. Of these Member States 16 provided us with a response to the questionnaire.

Country code	Member state	Implemented EC2006/32
AT	Austria	Yes
BE	Belgium	No
BG	Bulgaria	Yes
CY	Cyprus	Yes
CZ	Czech Republic	Yes
DK	Denmark	No
EE	Estonia	No
FI	Finland	Yes
FR	France	Yes
DE	Germany	Yes
GB	United Kingdom	Yes
GR	Greece	Yes
HU	Hungary	No
IE	Ireland	No

Country code	Member state	Implemented EC2006/32
IT	Italy	Yes
LV	Latvia	No
LT	Lithuania	Yes
LU	Luxembourg	No
MT	Malta	No
NL	Netherlands	Yes
PL	Poland	No
PT	Portugal	No
RO	Romania	No
SK	Slovakia	No
SI	Slovenia	Yes
ES	Spain	No
SE	Sweden	No

H.2. Questions

The analysis was performed on responses to the following set of questions. These questions were sent to all DPA representatives in the 27 member states.

#	Question
1.	To what extent has the European Directive on Energy saving (2006/32/EC) been implemented in your jurisdiction? Did your National Data Protection Authority submit any comments during the implementation process? What were they?
2.	Regarding Directive 95/46/EC, what is considered legitimate purpose(s) for collecting and processing of smart grid personal data? Data subject consent, smart grid law, or other. This question applies to the different data types; e.g. for monthly billing data the legitimate ground could be different than for 15 minute interval data.
3.	Who is considered to be the "data controller" (95/46/EC article 2) or data controllers jointly of the smart grid data processing (DSO, supplier, other)? Who is considered to be the "data processor"?
4.	How are the provisions of 95/46/EC article 6.1.e implemented: keep personal data no longer than is necessary for the purposes for which the data were collected or for which they are further processed. What appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use were laid down?
5.	How are the provisions of 95/46/EC article 11 implemented: in what way do data subjects need to be informed about the data processing?

6.	What is considered the legitimate ground for communicating smart grid personal data to external parties, e.g. suppliers, value added services?
7.	What data protection principles and measures have been incorporated in the national implementations - of Smart Grids, smart metering and energy end-use efficiency and energy services - to protect personal data, in particular:
7.1.	What are the differences between these implementations of data protection principles and measures?
7.2.	Are these principles and measures specifications of the local Data Protection Laws (DPL) or additions?
7.3.	If no or limited principles or measures have been incorporated, in what specific (other than DPL) laws and regulations are these covered (if any)?
7.4.	What other laws and regulations and guidelines apply?
7.5.	Are there any changes, additions, alterations needed in the local implementations of the 2006/32/EC in order to:
7.5.1.	Facilitate the implementation of smart meters / smart gird from a data protection point of view and reduce administrative burden (equal compliance standards for operators)?
7.5.2.	Protect citizens / consumers to establish a level playing field (equal level of protection for consumers)?
7.5.3.	How is supervision for compliance with energy directive (and in particular the privacy issues related) organised (supervising authority)?
7.5.4.	How consumer protection with regards to complaints of misuse is organised (Ombudsman)?
8.	Did your Member State implement a Privacy Risk Analysis approach on Smart Grids and smart metering data protection, and is a risk classification scheme included?
9.	What are your Member State specific Privacy Impact Assessment (PIA) standards and practices?
10.	Does your Member State actively promote the implementation of “privacy by design” principles? How?
11.	Does your Member State promote privacy certificates, if yes:
11.1.	how is the certification authority organized;
11.2.	how is certification financed;
11.3.	how do you deal with the potential dynamic environment (e.g., update of meter code, changes in the architecture, new services, etc).
12.	Which parts of the smart grid functionality must be executed in a Trusted Domain (e.g., tamper-proof hardware, or by a trusted service) through Member State legislation and/or the European MID (Measuring Instruments Directive)? Which parts are considered critical from a privacy point of view and need additional protection (considering article 8 of direction 95/46/EC)?