**FP7 Grant Agreement N° 607109**

***S*ecurity for smart *E*lectricity *GRID*s**

# D1.5 Report on analysis of policies regarding smart grid security

Due date of deliverable: 01/10/2015
Actual submission date: 30/06/2016
Workpackage: WP1 Use cases and security goals
Number of pages: 49
Revision: Version 1
Classification level: Public

| | |
|---|---|
| Project type: | Collaborative project – small or medium scale focused research project |
| Thematic Priority: | FP7-SEC-2013-1 |
| Start date of project: | October 1st, 2014 |
| Duration: | 36 months |

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

# Management summary

This document contains the results of an analysis on policies that relate to smartgrid security. A long list of policies were identified and part of those policies were analysed in more depth, using a analysis framework that is developed by SEGRID. The main observations are:

1. At European level, a harmonised approach to smart grid security is clearly lacking. Only a limited set of countries have developed security requirements for energy smart grid equipment and devices.
2. The understanding of smart grid security and other key terminology varies considerably from member state to member state. This influences the different approaches to smart grid security strategy among these member states.
3. Four areas are identified, that were not properly addressed in the analysed smart grid security policies: Shift of responsibilities from the transmission to the distribution level and the redefinition of the roles of the actors involved, the definition of the interface between the public grid and the consumer/prosumer, responsibilities for (cyber) security by new actors in the combined ICT-energy sector chain of operations (e.g. metering operators, electronic vehicle infrastructure operators and related financial services), the role of (cyber) security policies.
4. There exist many (security) directives, regulations, guidelines and standards which are applicable from a more generic point of view. This generic legislation, which addresses a wider domain, may apply to a specific area such as smart grid security as well. Implementation of generic legislation for the Smart Grid domain, however, requires interpretation.
5. Specific (cyber) security requirements for smart grids may be mandated by national lawmakers in e.g. energy grid (operations) acts. For smart grids in general, currently very few technical laws have been identified. Several nations have made specific laws, however, these apply only to the smart meter domain.
6. National law may mandate critical infrastructure operators to report cyber security breaches other than the data privacy affecting ones as well. However, it is unclear yet whether the lower distribution level parts of the smart grid will fall under the mandatory reporting mechanisms or not.
7. Penalisation of cyber-attacks on information systems in general mandates EU member states to sanction attacks on information systems, which may impact requirements regarding sanctions in the area of cyber-attacks on smart grids.
8. Current policies leave the impression that the lack of cyber security or the impact of cyber security vulnerabilities are confined only to the information communication systems of the Smart Grid. Potential cyber security vulnerabilities however, could apply to all areas of the Smart Grid, including the performance of physical equipment.

It can be concluded that this analysis is a solid base for further studies on how to ensure gaps within policies can be filled. In the follow-up work (D1.6), SEGRID will conduct a survey among European smart grid stakeholders, to investigate how they use the policies that are available, what they think of the effectiveness of these policies and what they see as gaps in this area. SEGRID will analyse the gaps in current policies and construct recommendations to policy-makers and makers of standards in the smart grid domain to fill these gaps.

| | |
|---|---|
| Author(s) | Ruben ten Hove (TNO)<br>Eric Luiijf (TNO)<br>Reinder Wolthuis (TNO) |
| Contributor(s) | Nuno Medeiros (EDP)<br>Johan Rambi (Alliander)<br>Marcial Valmorisco (INCODE) |
| Review | Judith Rossebø (ABB)<br>Francisco Melo (EDP) |

| **Security Assessment** | **See deliverables table for security assessment requirements** |
|---|---|
| Approval Date | 30/06/2016 |
| Remarks | None |

# TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT ..... 5
1.1 The SEGRID project objectives ..... 5
1.2 Work Package 1 – Use Cases and Security Goals ..... 6
1.3 Deliverable D1.5 - Report on analysis of policies regarding smart grid security ..... 7
1.4 The structure of Deliverable D1.5 ..... 8
2 ANALYSIS SCOPE, CONTENT AND FRAMEWORK ..... 8
2.1 Types of documents ..... 8
*2.1.1 International intergovernmental arrangements ..... 8*
*2.1.2 EU general and legislation documents ..... 9*
*2.1.3 Standards and Sector-specific frameworks ..... 10*
*2.1.4 Framework of national laws and regulations ..... 11*
2.2 Identification of documents ..... 12
2.3 Analysis framework ..... 16
3 ANALYSIS RESULTS AND CONCLUSIONS ..... 19
3.1 Observations and Conclusions ..... 19
3.2 Way forward ..... 21
4 GLOSSARY ..... 22
5 REFERENCES ..... 24
ANNEX A: COMPLETED ANALYSES ..... 25
ANNEX B: VARIOUS TYPES OF DOCUMENTS AND THEIR KEY CHARACTERISTICS ..... 45
ANNEX C: FULL LIST OF CONSIDERED DOCUMENTS ..... 47

# 1 Introduction – Rationale of this document

This section introduces the SEGRID project and defines the goals of this deliverable.

## 1.1 The SEGRID project objectives

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. In the coming years, the level of automation in electricity distribution grids will grow substantially. Smart meters will be deployed at home premises, and remote terminal units (RTUs) will be placed in distribution substations. The increased automation should provide a better view of how electricity flows to the medium and low voltage grids. It will provide grid operators increased control of that flow. But the increased automation also has major consequences for the cyber security of the enhanced electricity grid. Not only does it add new attack vectors through which cyber attackers can enter and attack the networks of grid operators, the automation also offers other possibilities to damage the electricity grid itself.

From a technical point of view, it is not sufficient to only consider all the different components in a Smart Grid separately; they will together form a truly integrated system-of-systems. Moreover, the Smart Grid will neither be completely owned, nor completely controlled, by a single power system operator. There will be many smart grid services and components that are operated by other organisations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new methods for connecting with various smart grid applications using a diverse set of communication channels, such as local connection interfaces, distributed web access, and smart apps on smart phones. A number of new cyber security issues become critical in this context.

This new utility-wide system (-of-systems) will not come into existence overnight; the smart grid will be composed of a mix of old, even legacy, and new components. Therefore, we look at the smart grid as a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain security, privacy and dependability of the smart grid as a whole. The required security solutions to cope with this situation range from improvements in current security, privacy and operational, technical and organisational measures to the introduction of new security and privacy paradigms.

The term 'Smart Grid' is used for a wide variety of developments related to the automation of electricity grid. Focusing on the efforts of the project, SEGRID will work on five concrete use cases, shown in Figure 1. These have been further elaborated in the deliverable D1.1 of the project [1]. The five SEGRID use cases are:

1. Smart meters used for on-line reading of consumption and technical data;
2. Load balancing renewable energy centrally;
3. Dynamic power management for smart homes, smart offices, and electric vehicles;
4. Load balancing renewable energy regionally (substation automation);
5. Automatic reconfiguration of the power grid.

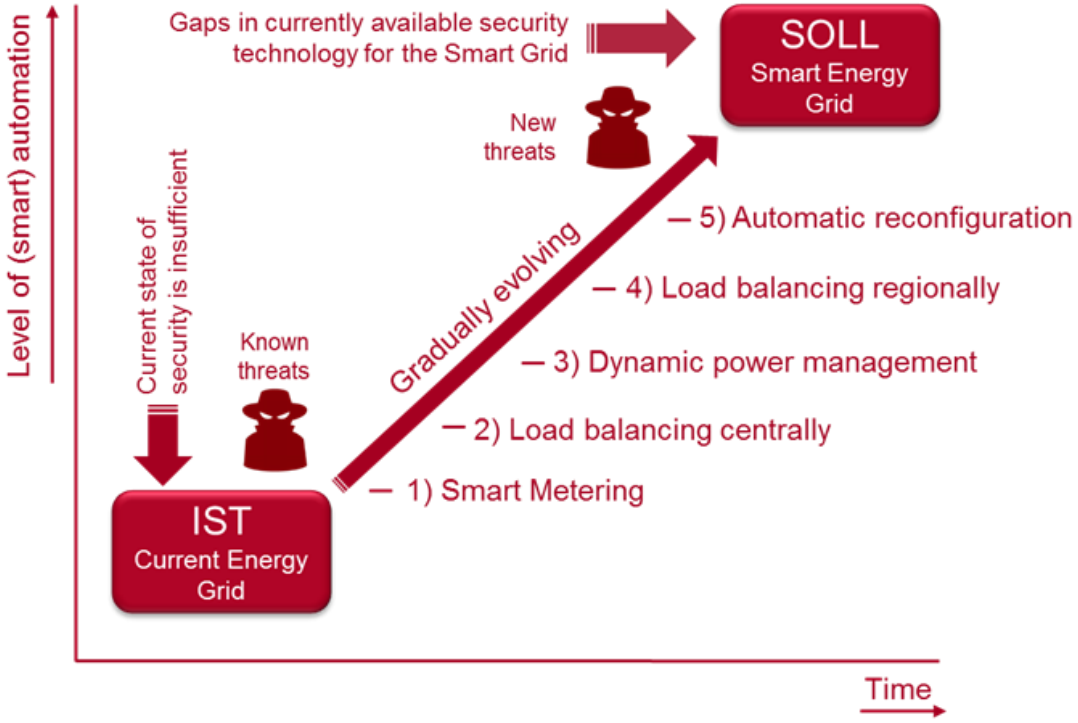


**Figure 1 SEGRID storyline**

The SEGRID use cases reflect important steps of the smart grid developments until 2020 and beyond. They cover the most relevant security and privacy issues that will arise from the increasing complexity of smart grids.

SEGRID will formulate privacy and security goals for these five use cases and perform a risk analysis of these use cases (WP2). Vulnerability assessment frameworks and tools to identify the risk in real systems will be developed (WP3), and gaps in the currently available security solutions will be identified (WP2). Solutions for some of these gaps will be developed in WP4. Selected vulnerability assessment tools and novel security solutions will then be tested in SITE (WP5).

## 1.2 Work Package 1 – Use Cases and Security Goals

Work Package 1 is a key building block for the SEGRID project, setting the basis for all activities within SEGRID.

The Work Package 1 main objectives are:

- Elaborate on the SEGRID reference architecture and describe the five use cases.
- Establish the security & privacy (S&P) goals for each of the SEGRID use cases.

- Identify points of improvement with respect to Smart Grid security and privacy in policies.
- Assess the cost of implementing security protection technologies that are developed in WP4 for each of the Smart Grids use cases.

## 1.3 Deliverable D1.5 - Report on analysis of policies regarding smart grid security

Deliverable D1.5 provides an analysis of policies regarding smart grid security and their applicability for different stakeholders.

Deliverable D1.5 is an outcome of Task T1.3. See also the task and deliverables dependency graph in Figure 2.

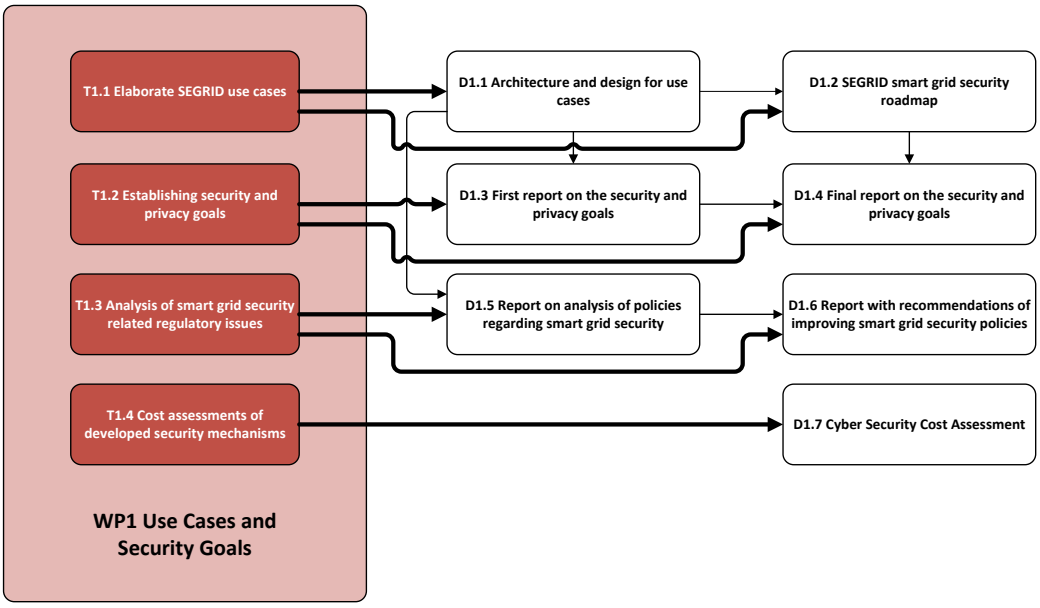


**Figure 2 - Dependencies in WP1**

The results of this deliverable will be verified and enriched by conducting a survey among relevant stakeholders. The results of the survey will be included in D1.6.

Based on the analysis in deliverable D1.5, the survey results, the results of D1.1 [1] and the findings in other SEGRID work packages, recommendations to improve smart grid security policies will be formulated in D1.6. These results will be used to support European standardisation bodies and regulators in their development of smart grid-related policies and regulations.

## 1.4 The structure of Deliverable D1.5

The deliverable is structured in three main sections and two annexes.

- Section 2 presents the analysis method, templates, and references to the documents used for this analysis of smart grid security and privacy policies. Also the rationale behind the choice of content and methods will be elaborated upon.
- Section 3 presents the statistical results from the combined analysis of documents, as well as preliminary conclusions on the currently available and analysed policy documents.
- Annex A contains the completed templates of all identified documents.
- Annex B contains a table outlining the distinctions between various types of documents, their purpose, mandatory, guidance or good practices, scope, etcetera.
- Annex C contains the full list of policy documents that were considered

# 2 Analysis scope, content and framework

In this section, we present the scope, content and framework used for the analysis of various cyber security and privacy-related policies across Europe with a possible relevancy to the SEGRID use cases.

## 2.1 Types of documents

For a good understanding of this deliverable, the differences in types of documents applicable to smart grids related to strategy, legislation, norms, standards, good practices, as well as their scope need to be understood. Some documents are binding, others are not. Some apply to all EU Member States, others to just a few, or are specific to the energy / smart grid sector and the manufacturers of Smart Grid components. To ensure consistency throughout this document, without having to specify the exact document type each time, the term policy will be used to refer to any document fitting any of the descriptions below. When required, a more specific term will be used. The descriptions of documents are grouped according to the following scopes:

- International intergovernmental agreements;
- EU general and legislative documents;
- (Energy/Smart Grid) standards and sector-specific frameworks;
- Framework of national laws and regulations.

### 2.1.1 International intergovernmental arrangements

#### Convention

A ‘convention’ is an international treaty which documents a number of articles. It is a formal agreement between States. The generic term ‘convention’ is thus synonymous with the generic term ‘treaty’. Conventions are normally open for participation by the international commu-

nity as a whole, or by a large number of States. Usually the instruments negotiated under the auspices of an international organization are entitled conventions. Nations have to transpose those articles into national law and regulations. Ratification by the nation's Parliament may be required. Articles may provide an "A. heavy" and a "B. lightweight" option. A nation has to declare which version they implement in their national law. An example is the Convention of Budapest (a.k.a. "Cybercrime Convention")[2]. Even when undersigned, each nation can have its own implementation pace before ratification.

### 2.1.2 EU general and legislation documents

#### Strategy

A "strategy" documents the strategic or strategic-tactical approach (by the EU) to a given issue or domain including the scope of Smart Grids. An EU strategy may be focused on the internal alignment of the EU, which are EU member states and the EU institutions and bodies ('internal'), or on the EU's approach to the world ('external'). A strategy may include or be accompanied by an action plan[3].

#### Regulation

A "regulation" is a binding legislative act with general application, issued by the European Council. A regulation must be applied in its entirety across all EU member states. A date is stated for when the regulation is to be applicable in all member states.

#### Directive

A "directive" is a legislative act that sets out a goal that all EU member states to which the directive is addressed must achieve.1 However, it is up to the individual EU member states to devise their own laws on how to reach these goals ("transposition of the directive"). Resulting national implementations may be stricter than the directive sets out, depending on national needs and political debate.

A proposed directive may be discussed and amended in one or more readings by the European Council and the European Parliament before being published as final. When published as final, a timetable is added stating the date of entering into force and the deadline for the member states to transpose the directive into national law and/or regulation. When a member state does not transpose a directive into national legislation in time or does that in an insufficient way, the European Commission may initiate legal action against the member state before the European Court of Justice.

#### Decision

A "decision" by the EU is binding only on those to whom it is addressed (e.g. an EU member state, an individual company or an organisation) and is directly in force.

[1] The legal basis for a Directive is article 288 of the Treaty on the Functioning of the EU (TFEU).

#### Recommendation

A "recommendation" is not binding. A recommendation allows the institutions of the EU to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.

#### Opinion

An "opinion" is an instrument that allows the institutions of the EU (Commission, Council, Parliament, the Committee of the Regions, the European Economic and Social Committee, and the European Data Protection Supervisor) to make a statement in a non-binding fashion, or in other words without imposing any legal obligation on those to whom it is addressed. While laws are being made, the committees give opinions from their specific regional, economic and social viewpoint(s).

#### Guideline

A "guideline" gives a more extensive help in how to apply regulation or a directive, for instance it provides some process steps for implementation.

### 2.1.3 Standards and Sector-specific frameworks

There exists a large score of 1) equipment-specific, 2) sector-specific, 3) national, 4) European and 5) international standardisation institutions. The following is a non-exhaustive list respectively:

- European Smart Meter Industry Group (ESMIG), International Society of Automation (ISA);
- Netbeheer Nederland, ENTSO-E (and e.g. NERC in the USA);
- BSI Group, NEN, DIN (and e.g. ANSI and NIST in the USA) - –national standardisation organisations[2];
- CEN, CENELEC – European standardisation organisations;
- ISO/IEC, ISO – International standardisation organisations.

One distinguishes [4]:

#### Norm (de jure standardisation)

A voluntary recognised agreement between stakeholders about specifications or criteria about a product, process, service, or a method which is developed through a process of normalisation. Norms have an (inter)national legal basis and may be mandated by law.

#### Standard (de facto standardisation)

A document with agreements, formalised good practices, specifications or criteria about a product, process, service, or a method which is developed through either a non-formal normalisation process or a closed process (company and consortium standards) or a process

[2] These national bodies take part in the standardisation processes of CEN/CENELEC and ISO.

without harmonisation by market force (e.g. GSM).
Standards may be open –meaning accessible to all- which stimulates interoperability.

#### Code of Conduct

A "Code of conduct" is a set of commonly agreed principles and expectations that are considered binding on the membership of a particular – in this case, a sector-specific – group of Smart Grid operators.

#### Good Practice

A "Good Practice" is a less formal de facto standard for (inter)operational processes by a closed community. A good practice can be regarded as a baseline for – in this case, a sector-specific – group of Smart Grid operators or Smart Grid sector-specific equipment manufacturers; one may use a higher level standard instead.

#### Recommendation

A "Recommendation" is non-binding and mostly considers a Good Practice that has been made public and transparent to a wider community.

#### Guideline

A "Guideline" is a (Smart Grid) sector-wide agreed Good Practice which gives a more extensive help in how to apply norms and standards.

### 2.1.4 Framework of national laws and regulations

The national framework of legislation distinguishes:

#### National Strategy

A "Strategy" documents the strategic or strategic-tactical approach by a member state to a given issue or domain, in this case within the scope of smart grids. A national strategy on Smart Grids may be focused on the internal alignment of the member state's government ('internal'), on the alignment of public-private and or public-private-academic/research communities' bodies, or on its alignment approach to the world ('external'). A strategy may include or be accompanied by an action plan [3].

#### Legislative act (a.k.a. 'law')

A legislative act is binding for all citizens and institutions. An act is proposed either by the Parliament or the government of a nation and become into force only after a parliamentary process.

#### Administrative decree (a.k.a. "regulation")

An administrative decree is binding to a constituency or (group of) citizens. A decree can be put into force by a sector-responsible Minister or a national regulator based upon the powers of Minister or regulator offered by the (Parliamentary supervised) legal mandate.

## 2.2 Identification of documents

For collecting documents relevant to our analysis, a scope was defined to limit the amount of documents to be analysed, and to ensure documents that were analysed are able to provide a clear view on the state of current policies.

- Non-EU documents were not analysed, because these are only relevant as inspiration of the gap analysis in D1.6.
- The topic focus is either security or privacy, but is always focused on smart grids.

The table below contains the characteristics that have been used to categorize each relevant policy document:

- *The type* - Depicts the type of document. A subset of the list in 2.1 are is used in the categorization, because we did not find documents of all types that were describe in 2.1. Moreover, some types of documents are only relevant for the gap analysis in D1.6.
- *Date of publication* – The date that the document was published
- *Geographical scope* – Either EU or national. The analysis of policies was not limited to EU level policies but also some national policies were included. Policies outside the EU were not analysed, but will be used to find gaps in existing European policies, which is reported in deliverable D1.6.
- *Topic focus* – either privacy related, security related or both (generic)
- *Domain* – The specific domain that the document relates to. Each document relates to one or more domains. The domain axis of the SGAM model was used as a basis, where the Energy supplier and data hub domain were added, based on the granularity of domains in D1.1 [1]. In D1.1, Energy supplier and Data hub were seen as two separate domains, but in the context of this document this separation does not add value and we will consider these as one domain. This extra domain was not added during a first iteration of the analysis. Therefore, some documents have not been scored with respect to this domain, since these were not relevant to require an additional analysis.

**Table 1: Characteristics of policies**

| *Characteristic* | *Options* |
|---|---|
| **Type** | Law<br>Code of conduct<br>Directive<br>Regulation<br>Standard<br>Good practice<br>Guideline<br>National strategy |
| **Date of publication** | *Date* |
| **Geographical scope** | EU<br>National |
| **Topic focus** | Generic<br>Privacy<br>Security |
| **Domain** | Generation<br>Transmission<br>Distribution<br>DER<br>Energy supplier and data hub<br>Customer |

The documents that were found and fully analysed are shown in table 2. A full list of documents that were considered can be found in Annex C. The numbering is according to the full list, and therefore not continuous in the list of table 2. The full list of documents is retained for use in D1.6, and to provide a full overview of the results of our search.

**Table 2: list of policies that were analysed**

| # | Title |
|---|---|
| **2** | Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities |
| **4** | Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision |
| **5** | Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union |
| **13** | Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Smart Grids: from innovation to deployment |
| **14** | Smart grid security certification in Europe: Challenges and recommendations |
| **15** | CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Information Security |
| **16** | Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection |
| **17** | Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" |
| **19** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the |

| | |
|---|---|
| | protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) |
| **22** | Cyber Security Information Sharing Act |
| **23** | Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications |
| **27** | Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA |
| **28** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). |
| **31** | Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid (Cbp) (Obligation to report breaches of personal data and expansion of the authority of the Dutch regulator for the protection of personal data to impose penalties.) |
| **32** | Dutch law that allow consumers to OPT-OUT: refuse a smart meter's communication function [5], art 26ac lid 2 |
| **33** | Gedragscode: Verwerking door elektriciteits- en gasleveranciers en door de onder hun verantwoordelijkheid handelende meetbedrijven van op Kleinverbruikers betrekking hebbende Persoonlijke Meetgegevens afkomstig uit Slimme Meters (Code of conduct: processing by electricity and gas suppliers and their suppliers of personal measurement data that originates from smartmeters of retail consumers) |
| **34** | Aanbeveling over na te leven beginselen bij smart grids en slimme meters (CO-AR-2011-004) (Recommendations about principles to be applied for smart meters and smart grids]), Belgian Commission For Data Protection |
| **35** | Obligation to update the application and system software of smart meters in case the manufacturer requires that [5], art 26ac |
| **40** | Law 24/2103 on the electric sector |
| **41** | Royal Decree 1955/2000 |
| **42** | Riordino del settore energetico, nonche' delega al Governo per il riassetto delle disposizioni vigenti in materia di energia (Reforming the energy sector as well as delegation to the government to reform the current rules on energy) |
| **43** | Legislative Decree No 387 of 29 December 2003 |
| **44** | Article 7 which implements Directive 2012/27/EU |
| **49** | Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC |
| **50** | Energy Independence and Security Act, VS, Section 1301 (2007) |
| **51** | Roadmap Smart Grids (English Version) |
| **52** | Smart Grid Strategy: The intelligent energy system of the future |

Table 3 shows a numbered list related to the list above, with the characteristics of each document. These categorize the documents

**Table 3: Characteristics of each policy**

| # | Type | Date of publication | Geographical scope | Topic focus | Domain |
|---|---|---|---|---|---|
| **2** | Directive | 7-3-2002 | EU | Security | Generation, Transmission, Distribution, DER, Customer |
| **4** | Directive | 12-8-2013 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **5** | Directive | 18-12-2015 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **13** | Guideline | 4-12-2011 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **14** | Guideline | 1-12-2014 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub |
| **15** | Guideline | 1-11-2012 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub |
| **16** | Directive | 12-8-2008 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub |
| **17** | Guideline | 30-3-2009 | EU | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub |
| **19** | Regulation | 27-4-2016 | EU | Privacy | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **22** | Law | 1-12-2015 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **23** | Regulation | 24-6-2013 | EU | Privacy | Distribution, DER, Energy supplier, Data hub, Customer |
| **27** | Directive | 27-4-2016 | EU | Security | Distribution, DER, Energy supplier, Data hub, Customer |
| **28** | Regulation | 27-4-2016 | EU | Security | Distribution, DER, Energy supplier, Data hub, Customer |
| **31** | Law | 10-2-2015 | National | Security | Distribution, DER, Energy supplier, Data hub |
| **32** | Law | 22-2-2011 | National | Privacy | Energy supplier, Data hub, Customer |
| **33** | Code of conduct | 8-1-2013 | National | Privacy | Energy supplier, Data hub, Customer |
| **34** | Recommendation | 15-11-2011 | National | Privacy | Distribution, DER, Customer |
| **35** | Law | 22-2-2011 | National | Privacy | Distribution, DER, Customer |
| **40** | Law | 27-12-2013 | National | Security | Generation, Transmission, Distribution, DER, Customer |

| | | | | | |
|---|---|---|---|---|---|
| **41** | Law | 1-12-2000 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **42** | Law | 13-9-2004 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **43** | Law | 29-12-2003 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **44** | Law | 1-1-2013 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **49** | Directive | 25-10-2012 | EU | Privacy | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |
| **50** | Policy | 19-12-2007 | National | Security | Transmission, Distribution, DER |
| **51** | Policy | 11-2-2012 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub |
| **52** | National strategy | 1-5-2015 | National | Security | Generation, Transmission, Distribution, DER, Energy supplier, Data hub, Customer |

## 2.3 Analysis framework

The policies that were identified in section 2.2 were analysed and scored according to several criteria. Each of these criteria used a scale of 1 to 5, where the scores 1, 3 and 5 are defined to ensure consistency between analysts. The scores 2 and 4 allow to provide nuance in the scoring, and makes the scale re-usable for the survey which is to be conducted for D1.6. Applicability is not found in the table, but is scored by giving a score when a document is applicable to a certain domain. If it is not applicable, it isn't scored and can thus be ignored in that domain.

For each of the criteria, a short explanation was provided on why a certain score was given. For this analysis, the template as shown in table 4 was used. In Annex A, the detailed outcome of the analysis can be found. Each policy has been analysed using the framework, and if applicable or noteworthy, further comments were made to explain its relevance to the analysis.

**Table 4: Policy document analysis template**

| #: | Title: | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Energy suppli-er & data hub*[3] | *Customer* | *Explanation* |
| **Effective-ness** | | | | | | | |
| **Strictness** | | | | | | | |
| **Practica-bility** | | | | | | | |
| **Sustaina-bility** | | | | | | | |
| **Conflicting** | | | | | | | |

The following outlines the scoring indicators for scoring the documents per criterion.

*Effectiveness*: How well does the policy ensure it will have its intended effects?

Scoring:

1. The policy has its objectives defined, but barely describes methods on how to effectuate these policies.
3. The policy has its objectives well defined, and describes methods on how to effectuate these policies, but leaves much room for interpretation of these objectives.
5. The policy has its objectives well defined, and describes methods on how to effectively apply these while ensuring these objectives will be met.

*Strictness*: What level of detail is required by the policy in the application of its objectives?

Scoring:

1. The policy leaves much room for interpretation, and uses broad terms to define its objectives and how these should be met.
3. The policy defines boundaries on the implementation, and describes several qualitative measures on how to achieve its objectives.
5. The policy barely leaves room for interpretation, and ensures objectives can be tested and measured to ensure if these are met.

[3] Abbreviated to ES & DH in Annex A for brevity

*Practicability*: What is the practicability of implementing the policy? (regarding cost, time, etc.)

Scoring:

1. The policy asks for improbable timelines and has unclear or unrealistic expectations of the cost of achieving its objectives.
3. The policy has set requirements that can be achieved, but does rely on unclear assumptions.
5. The policy takes cost and time into account, and gives clear indication into the possible requirements regarding practical issues.

*Sustainability*: What is the ability of the policy to sustain its effectiveness in the long term?

Scoring:

1. The policy does not provide means to ensure its effectiveness in the long term.
3. The policy provides means to ensure its effectiveness in the long term, yet provides little indication on what might be causes to lose its effectiveness.
5. The policy is clear on how to sustain effectiveness, and provides guidelines on how to ensure sustaining the effectiveness.

*Conflicting*: To what degree does this policy conflict with other policies?

Scoring:

1. The policy has no conflicting policies.
3. The policy may be hindered by several policies.
5. The policy seems unable to be applied (in certain regions) due to clear conflicting objectives.

# 3 Analysis results and conclusions

The policies that were collected and analysed in this report can be seen as a sufficient representation of currently available policies regarding security and privacy for smart grids. The analysis of these documents has provided several conclusions regarding use and effectiveness of current available policies on privacy and security in Smart Grids. The conclusions are depicted below.

## 3.1 Observations and Conclusions

1. At European level, a harmonised approach to smart grid security is clearly lacking. Only a limited set of countries have developed security requirements for energy smart grid equipment and devices. These initiatives have been developed in order to meet specific national energy smart grid needs and diverse energy regulatory requirements. This produces diversity in the specifications for security requirements and the lack of common understandings and approaches between member states may hamper international cooperation, a need which is acknowledged by all member states and beyond.
2. The understanding of smart grid security and other key terminology varies considerably from member state to member state. This influences the different approaches to smart grid security strategy among these member states.
3. Four areas are identified, that were not properly addressed in the analysed smart grid security policies:
    - Shift of responsibilities from the transmission to the distribution level and the re-definition of the roles of the actors involved.
    - The definition of the interface between the public grid and the consumer/prosumer.
    - Responsibilities for (cyber) security by new actors in the combined ICT-energy sector chain of operations, e.g. metering operators (ESCo), electronic vehicle infrastructure operators and related financial services.
    - The role of (cyber) security policies.
4. There exist many (security) directives, regulations, guidelines and standards which are applicable from a more generic point of view. This generic legislation, which addresses a wider domain, may apply to a specific area such as smart grid security as well. Implementation of generic legislation for the Smart Grid domain, however, requires interpretation. This may be found in EU-level opinions [document 29], recommendations by national authorities [document 34] and sector-wide code of conducts / good practices [document 33]. For instance, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) can be considered as such a type of legislation which will apply as a baseline for the data protection in the wider Smart Grid scope but mainly to the prosumer/consumer area in the smart grid domain. This may drive the need for security and privacy protection requirements for smart grid in general. However, this will be limited to those components where data of individuals / households / customers is being pro-

cessed, transmitted and stored. Apart from the current focus area of smart meters and in some cases (e.g. [document 34]) smart appliances in homes and small businesses, this may apply also for other smart grid components in the area of data concentrators, meter information processors, smart fine-grain power distribution devices (DSOs) and DER equipment. The GDPR, which becomes effective as of May 25, 2018, and its predecessor Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, drives the opinions, recommendations and good practices in specific domains [document 28]. Moreover, some EU nations like The Netherlands have developed laws and regulations about the mandatory reporting of cyber security breaches when it concerns data protection issues [document 31] in anticipation of the GDPR.

5. Specific (cyber) security requirements for smart grids may be mandated by national lawmakers in e.g. energy grid (operations) acts. For smart grids in general, currently very few technical laws have been identified. Several nations have made specific laws, however, these apply only to the smart meter domain. The Netherlands provides energy grid customers with the possibility to opt-out remote communication of smart meters [document 32], and the obligation for the power grid operator to patch/update smart meter software in case a smart meter manufacturer requires that [document 35]. This type of obligation for an operator (e.g. TSO, DSO, DER) to update application or system software in case the manufacturer states the need, is a "policy gap" for smart grid components in general. This will be carried forward to deliverable D1.6 as a European level policy need.
6. National law may mandate critical infrastructure operators to report cyber security breaches other than the data privacy affecting ones as well. However, it is unclear yet whether the lower distribution level parts of the smart grid will fall under the mandatory reporting mechanisms or not (see e.g. [document 54]). This type of obligation for operators (e.g. TSOs, DSOs, DERs, ENSOs) to report cyber security breaches of smart grids to the designated authority is an identified "policy gap" in the smart grid components in general. A cyber security breach may affect the wider European area and therefore be a risk to the European economy and society. This will be carried forward to deliverable D1.6 as a European level policy need.
7. Penalisation of cyber-attacks on information systems in general [document 4] mandates EU member states to sanction attacks on information systems, which may impact requirements regarding sanctions in the area of cyber attacks on smart grids.
8. Current policies leave the impression that the lack of cyber security or the impact of cyber security vulnerabilities are confined only to the information communication systems of the Smart Grid. Potential cyber security vulnerabilities however, could apply to all areas of the Smart Grid, including the performance of physical equipment. That is, cyber security implications can materially impact the industry's ability to provide commands that result in a physical action (i.e. the opening or closing of a switch). Therefore, policies definition for cyber security must include more than just those elements that are linked to the information and communication systems.

## 3.2 Way forward

It can be concluded that this analysis is a solid base for further studies on how to ensure gaps within policies can be filled. The various policies that were analysed may uncover gaps and other aspects which will be considered by deliverable D1.6 for consideration as recommendation to policy-makers and makers of standards in the smart grid domain. Also SEGRID will conduct a survey among European smart grid stakeholders, to investigate how they use the policies that are available, what they think of the effectiveness of these policies and what they see as gaps in this area.

# 4 Glossary

This glossary serves as inventory of technical terms and abbreviations used in the document. For detailed background information on cryptographic primitives or testing procedures we refer to the referenced literature.

| | |
|---|---|
| **CEN** | European Committee for Standardization |
| **CENELEC** | European Committee for Electrotechnical Standardization |
| **CSO** | Charge Spot Operator |
| **DC** | Data Concentrator |
| **DER** | Distributed Energy Resources |
| **DMS** | Distribution Management System |
| **DSO** | Distribution System Operator |
| **Dx.y** | Deliverable x.y |
| **EMS** | Energy Management System |
| **EMSP** | Electro Mobility Service Provider |
| **ETSI** | European Telecommunications Standards Institute |
| **EV** | Electric Vehicle |
| **G3** | Alliance for PLC technology |
| **GIS** | Geographical Information System |
| **GPRS** | General Packet Radio Service |
| **GUI** | Graphical User Interface |
| **HAN** | Home Area Network |
| **HES** | Head-End System |
| **HMI** | Human Machine Interface |
| **HV** | High Voltage |
| **IEC** | International Electrotechnical Commission (ISO) |
| **IED** | Intelligent Field Device |
| **ISO** | International Organization for Standardization |
| **LAN** | Local Area Network |
| **LN** | Local Network |
| **LV** | Low Voltage |
| **MDMS** | Meter Data Management System |
| **Meter** | The term "meter" refers unless stated otherwise to the electricity meter. When necessary the document distinguishes between electricity meter and utility meter. |
| **MV** | Medium (level) Voltage |
| **micro-CHP** | Micro combined heat and power |
| **NN** | Neighbouring Network |
| **OMS** | Outage Management System |
| **OSCP** | Open Smart Charging Protocol |
| **OSGP** | Open Smart Grid Protocol |
| **OSI model** | The ISO Basic Reference Model for Open Systems Interconnection. |
| **PLC** | Power Line Communication |

| | |
|---|---|
| **PQ** | Power Quality |
| **PV** | Photovoltaic |
| **RTU** | Remote Terminal Unit |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SE** | Secure Element |
| **SEGRID** | *S*ecurity for smart *E*lectricity *GRID*s |
| **SGAM** | Smart Grid Architecture Model |
| **SG-CG** | Smart Grid Coordination Group (CEN/CENELEC, ETSI) |
| **SMITP** | Smart metering Information and Telecommunication Protocol |
| **TSO** | Transmission System Operator |
| **Tx.y** | Task w.y |
| **UMTS** | Universal Mobile Telecommunications System |
| **Utility meter** | Meter for, e.g., power, gas, water, and heat consumption. |
| **WAN** | Wide Area Network |
| **WPx.y** | Work Package x.y |
| **3G / 4 G** | Third/ Forth generation mobile communication. |

# 5 References

[1] WP1 SEGRID, 'D1.1 Architecture and design for use cases', 2015.
[2] 'Details of Treaty No.185'. [Online]. Available: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[3] E. Luiijf, K. Besseling, and P. de Graaf, 'Nineteen national cyber security strategies', vol. 9, 2013.
[4] Forum Standaardisatie, 'Tekstvoorstel voor publicatie over Internationale standaardisatie van onbekende auteur(s)', vol. 1, pp. 1–20
[5] Elektriciteitswet http://wetten.overheid.nl/BWBR0009755/2016-04-01

# Annex A: Completed analyses

The following tables show the detailed results of the analysis of policy documents. Several documents were accompanied with further explanations if these were found to be valuable to the analysis.

| #: 2 | Title: Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities | | | | | |
|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 1 | 1 | 1 | 1 | 1 | High level principles |
| **Strictness** | 1 | 1 | 1 | 1 | 1 | High level principles |
| **Practicability** | 1 | 1 | 1 | 1 | 1 | High level principles |
| **Sustainability** | 1 | 1 | 1 | 1 | 1 | High level principles |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | High level principles |

| #: 4 | Title: Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | ES & DH | *Explanation* |
| **Effectiveness** | 1 | 1 | 1 | 1 | 1 | 1 | |
| **Strictness** | 5 | 5 | 5 | 5 | 5 | 5 | Concrete sanctions on attacks |
| **Practicability** | 1 | 1 | 1 | 1 | 1 | 1 | |
| **Sustainability** | 1 | 1 | 1 | 1 | 1 | 1 | |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | |

| #: 5 | Title: Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final |
|---|---|

| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | ES & DH | *Explanation* |
|---|---|---|---|---|---|---|---|
| **Effectiveness** | 3 | 3 | 3 | 3 | 3 | 3 | NIS has well defined objectives, describes methods but leaves room for interpretation |
| **Strictness** | 1 | 1 | 1 | 1 | 1 | 1 | The question 'what' to do is described well, but the question 'how' to do it is not addressed |
| **Practicability** | 3 | 3 | 3 | 3 | 3 | 3 | NIS has well defined objectives, describes methods but leaves room for interpretation |
| **Sustainability** | 3 | 3 | 3 | 3 | 3 | 3 | NIS has well defined objectives, describes methods but leaves room for interpretation |
| **Conflicting** | 3 | 3 | 3 | 3 | 3 | 3 | May conflict with GDPR around incidents (e.g. to which authorities?) |

| **#: 13** | **Title: Communication from the Commission to the European Parliament - Smart Grids from innovation to deployment** | | | | | | |
|---|---|---|---|---|---|---|---|
| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 5 | 5 | 5 | 5 | 5 | 4 | The policy describes the objectives well and also how to effectively meet these objectives with different methods of approach.<br>For customers, a short objective has been mentioned in this policy with a quick overview of how to meet this objective. |
| **Strictness** | 4 | 4 | 4 | 4 | 4 | 4 | The policy describes the different approaches to meet the objectives and not much room for interpretation is left, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | though there is some interpretation left. |
| **Practicability** | 4 | 4 | 4 | 4 | 4 | 4 | The objectives set in this policy are clear as well as the methods to meet them. The assumptions are clear, yet the timeline seems a bit short sometimes, but not necessary undo-able. |
| **Sustainability** | 1 | 1 | 1 | 1 | 1 | 2 | This policy does not provide any information in regards to sustaining its effectiveness in the long term.<br>For customers, it is mentioned shortly that if the requirements are not implemented correctly or if they are not effective, further action will be taken, possibly in its review of the Energy Services Directive. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | This policy has no conflicting policies. |

| **#: 14** | **Title: Smart grid security certification in Europe - Challenges and recommendations** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 5 | 5 | 5 | 5 | 1 | 0 | The policy sufficiently describes its objectives (*Harmonised European smart grid certification practices which cover the complete smart grid supply chain*) and the methods used to ensure these objectives will be met.<br>In this policy it's briefly mentioned that certification in smart grid cyber security also delivers a competitive advantage for both suppliers and service providers. It does not however describe methods to meet this objective. |
| **Strictness** | 3 | 3 | 3 | 3 | 1 | 0 | The policies describes several recommendations to implement, but leaves interpretation open for the parties that |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | actually need to act.<br>For energy suppliers no information is given about the boundaries on the implementation and only a vague objective is given, which creates much room for interpretation on how to meet it. |
| **Practicability** | 4 | 4 | 4 | 4 | 2 | 0 | The policy takes time and cost into account, but does not give specifics other than that it will be implemented soon and that it must be implemented in the current environment to avoid adding security later to existing systems and therefore incurring more costs.<br>For suppliers it is said that this policy will help to create more of a competitive advantage for both supplier and service provider. Though it is unclear how and if the policy really has this effect. |
| **Sustainability** | 5 | 5 | 5 | 5 | 5 | 0 | The policy has clear recommendations on how to sustain its effectiveness in the long term by building in flexibility and having a specific owner that ensures that this flexibility remains. This in turn should create a more competitive advantage for suppliers, both for the short term as well as the long term. |
| **Conflicting** | 3 | 3 | 3 | 3 | 1 | 0 | This policy may be hindered by several policies as this policy provides a framework for harmonised European Smart Grid Certification that covers the entire smart grid supply chain. Some policies do conflict with each other and might make the realisation of this policy more difficult. However an approach can be outlined that describes how to go from the current fragmented situation to a more harmonised one at the EU level. This approach allows for |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | adopting national specific approaches and requirements, while providing possibilities to adopt European based requirements to facilitate harmonisation, and benefit from joint standardisation efforts.<br>For energy suppliers this document has no conflicting documents. |

| **#: 15** | **Title: CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 3 | 3 | 3 | 3 | 3 | 0 | The policy has a well defined objective (*develop or update a set of consistent standards within a common European framework […] that will achieve interoperability […]… )* and method (The SGIS Toolbox ) to meet this objective. However, there is a lot of room for interpretation in how to use the toolbox to meet the objective. It does provides a general framework for risk analysis that can be used as a solid basis, from which deviation is possible following user and standardization needs. The SGIS Toolbox will help in identifying which standards can be used in Europe today and in the future and systematically identifying gaps in existing SGIS standards. This toolbox can be used for all domains except for the customer-domain. |
| **Strictness** | 3 | 3 | 3 | 3 | 3 | 0 | The policy describes the boundaries of the implementation tool (in this case the SGIS Toolbox) but leaves room for interpretation in how to use it. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Practicability** | 4 | 4 | 4 | 4 | 4 | 0 | The policy shows that the standards needed to establish the basis for Smart Grid Information Security are available today, but nevertheless there is a need for enhancement and for additional standards to integrate Smart Grid specific needs with a particular attention paid to implementing them in organizations and in system components in order to guarantee interoperability. It also describes that maintaining this policy requires continuous effort and that the toolbox is a valuable tool but it needs to be further developed and maintained so it can be used to reach the objective. |
| **Sustainability** | 2 | 2 | 2 | 2 | 2 | 0 | The policy describes that it will continuously update and improve the toolbox needed to meet their objective, however it does not say with what means, who will do it etc. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 0 | The policy provides no information regarding conflicting policies. |

| **#: 16** | **Title: Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 5 | 5 | 5 | 5 | 5 | 0 | The policy has a clear objective (*identification and designation of European critical infrastructures and the assessment of the need to improve their protection*) and describes clearly how to meet this objective via a set of procedures. |
| **Strictness** | 4 | 4 | 4 | 4 | 4 | 0 | The policy describes well defined methods on how to achieve the objective, though it still leaves some room |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | for interpretation on how to fulfil those methods. |
| **Practicability** | 3 | 3 | 3 | 3 | 3 | 0 | The policy describes that Member States shall take the necessary measures to comply with this directive by 12th January 2011. It does not, however, describe the costs that may be involved and/or give any other criteria in regards to the practicability of this directive. |
| **Sustainability** | 2 | 2 | 2 | 2 | 2 | 0 | The policy does not describe any means to sustain its effectiveness on the long term. It does however mention that this directive is the first step in a step-by-step approach to identify and designate European Critical Infrastructures and assess the need to improve their protection. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 0 | This policy gives no information in terms of conflicting with other policies. |

| **#: 17** | **Title: Communication from the Commission to the EuropeanParliament, the council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 5 | 5 | 5 | 5 | 5 | 0 | The policy describes a clear objective (*enhancement of the security and resilience of Critical Information Infrastructure to reap the full benefits of the information society*) and an action plan complete with different approaches on how to achieve and meet the objective. |
| **Strictness** | 4 | 4 | 4 | 4 | 4 | 0 | The policy defines clear approaches for |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | reaching the objective, but leave a little bit of room for interpretation on how to fulfil those approaches. |
| **Practicability** | 4 | 4 | 4 | 4 | 4 | 0 | The policy gives, for every approach, a target to meet, e.g. for the first approach of the action plan, the target is set to the end of 2010 for agreeing on minimum standards; end of 2011 for establishing well-functioning National/Governmental CERTS in all Member States. It does not give any information about costs. |
| **Sustainability** | 3 | 3 | 3 | 3 | 3 | 0 | The policy describes that enhancing the security and resilience of CIIs is a long term objective whose strategy and measures need regular assessments. Therefore, the Commission initiated a stock-taking exercise at the end of 2010 to evaluate the first phase of actions and to identify and propose further measures. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 0 | No information is given in the policy regarding conflicts with other policies. |
| This document mainly describes the information protection of the ICT sector and the Internet in general. It does not give enough information about Smart Grid Security, the energy domain or its stakeholders and this document therefore does not fall in the scope of SEGRID. | | | | | | | |

| **#: 19** | **Title: Regulation (eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 0 | 0 | 5 | 5 | 5 | 5 | The regulation describes a clear objective (*rules relating to the protection of natural persons with regard to the processing of per-* |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | *sonal data and free movement of personal data*) and defines several ways to meet this objective. |
| **Strictness** | 0 | 0 | 5 | 5 | 5 | 5 | The methods to meet the objective are defined in detail and little room for interpretation is left. This regulation describes specifically what can be done in regards to the protection and processing of personal data and which consequences there are if one does not comply with them. |
| **Practicability** | 0 | 0 | 4 | 4 | 4 | 4 | This regulation has set a reasonable timeline (May 2018) to implement and comply with all the rules stated in this regulation. It does not show specifics about costs though. It also describes which steps need to be taken to protect and process personal data. |
| **Sustainability** | 0 | 0 | 5 | 5 | 5 | 5 | This regulation has clearly defined how to sustain its effectiveness in the long term by describing that from 2020 and every four years thereafter, an evaluation and review of this regulation shall be done and the reports shall be made public. These reports shall then be examined to see if the regulation is still functional and applicable to that current situation. |
| **Conflicting** | 0 | 0 | 2 | 2 | 2 | 1 | This regulation does not conflict with other policies, although it does have a close relationship with Directive 2002/58/EC in regards to obligations on natural and legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union. This regulation will therefore not impose additional obligation that have already been set out in Directive |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | 2002/58/EC.<br>For customers this regulation does not conflict with other policies. |

| #: 22 | Cyber Security Information Sharing Act | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
| **Effectiveness** | 3 | 3 | 3 | 3 | 3 | 0 | This law describes a clear objective ("*sharing cyber security information*") but leaves much room open for interpretations of the methods to meet this objective. In addition, it is generic for Cyber Security of Information Sharing and therefore covering all the domains that are responsible for sharing information. |
| **Strictness** | 2 | 2 | 2 | 2 | 2 | 0 | This law uses broad terms to define its methods and how to meet the objective. |
| **Practicability** | 3 | 3 | 3 | 3 | 3 | 0 | The requirements set in this law can be achieved and implemented, although it is not clearly stated how much time and costs it will involve. |
| **Sustainability** | 1 | 1 | 1 | 1 | 1 | 1 | This law does not describe any means to ensure its effectiveness in the long term. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | This law has no conflict with any other policy document as it also states the following: "*Nothing in this title shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government*". |

| #: 23 | Title: Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications |
|---|---|

| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | ES & DH | *Customer* | *Explanation* |
|---|---|---|---|---|---|---|---|
| **Effectiveness** | 0 | 0 | 5 | 5 | 5 | 5 | The regulation has clear objectives (notification to national authorities and its subscribers in case of a personal data breach) and well defined methods to meet these objectives. |
| **Strictness** | 0 | 0 | 5 | 5 | 5 | 5 | This regulation has set very clear instructions on what to do in case of a personal data breach. These actions are mandatory for the provider. The attachments to this regulation describe the precise steps and information that are required. |
| **Practicability** | 0 | 0 | 4 | 4 | 4 | 4 | This regulation describes clearly when it will enter into force and what is expected from the Member States when it is in effect. It does not give any information regarding costs though. |
| **Sustainability** | 0 | 0 | 5 | 5 | 5 | 5 | This regulation describes clearly that it will be reviewed three years after the entry into force of the regulation and that its effectiveness and its impact on providers, subscribers and individuals will be evaluated. |
| **Conflicting** | 0 | 0 | 2 | 2 | 2 | 2 | This regulation does not have a conflict with other policies, but it does share its content with Directive 2002/58/EC. For example, implementing technical measures for the protection against data breaches are not discussed in this Regulation as they are already discussed in Directive 2002/58/EC. |

**#: 27 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, in-**

| vestigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 0 | 0 | 5 | 5 | 5 | 5 | |
| **Strictness** | 0 | 0 | 4 | 4 | 4 | 4 | Transposition leaves some room for flexibility / interpretation |
| **Practicability** | 0 | 0 | 5 | 5 | 5 | 5 | |
| **Sustainability** | 0 | 0 | 5 | 5 | 5 | 5 | |
| **Conflicting** | 0 | 0 | 1 | 1 | 1 | 1 | Conflicts are described and taken care of |
| **Published 04.05.2016 - entered into force on 24 May 2016, to be transposed to national law by 06.05.2018** | | | | | | | |

| **#: 28** | **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 0 | 0 | 5 | 5 | 5 | 5 | * The customers get at set of rights; the others obligations. |
| **Strictness** | 0 | 0 | 5 | 5 | 5 | 5 | |
| **Practicability** | 0 | 0 | 5 | 5 | 5 | 5 | Not only costs now, but one has to take into account and adapt to technological developments |
| **Sustainability** | 0 | 0 | 5 | 5 | 5 | 5 | one has to take into account and adapt to technological developments |
| **Conflicting** | 0 | 0 | 1 | 1 | 1 | 0 | |
| **Entered into force on 24 May 2016, it shall apply from 25 May 2018; supersedes the 95/46/EC Privacy regulation** | | | | | | | |

| #: 31 | Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid (Cbp) (Obligation to report breaches of personal data and expansion of the authority of the Dutch regulator for the protection of personal data to impose penalties.) INTO FORCE: 1-1-2016 | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 0 | 0 | 5 | 5 | 5 | 0 | It is a law plus memorandum discussing the background<br>Uncertain whether it applies to scenarios for DER which involve consumer/customer privacy data; if so, it will apply (5), otherwise no (0) |
| **Strictness** | 0 | 0 | 5 | 5 | 5 | 0 | The only interpretation is the freedom of the Data Protection Authority to select the height of the fine |
| **Practicability** | 0 | 0 | 5 | 5 | 5 | 0 | It seems to be working; first fines charged. |
| **Sustainability** | 0 | 0 | | | | 0 | A score cannot be given as the implementation by the regulator and costs/efforts involved are not a part of the policy |
| **Conflicting** | 0 | 0 | 2 | 2 | 2 | 0 | The law was in its design in conflict with Telcom package 13A and Financial services law. In its current form there is no conflict. It may be in conflict with the security breach reporting for CI law proposal. |
| Change to the Data Protection Law and other laws w.r.t. breach of security measures<br>- Organisations have to report data breaches both to te regulator and the individual affected customers when it concerns data protection (privacy) sensitive systems and data.<br>- The Privacy Authority is mandated to raise fines in case of breaches. | | | | | | | |

| #: 32 | Title: Dutch law that allows consumers to OPT-OUT: refuse a smart meter's communication function [Elektriciteitswet art 26ac lid 2] |
|---|---|

| *Domain* | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
|---|---|---|---|---|---|---|---|
| **Effectiveness** | 0 | 0 | 0 | 5 | 0 | 5 | |
| **Strictness** | 0 | 0 | 0 | 5 | 0 | 5 | |
| **Practicability** | 0 | 0 | 0 | 4 | 0 | 4 | Although DSO wants 100% remote access, current opt-out policy is a practical approach to avoid lengthy juridical processes. |
| **Sustainability** | 0 | 0 | 0 | 0 | 0 | 0 | |
| **Conflicting** | 0 | 0 | 0 | 0 | 0 | 0 | |

**#: 33 Gedragscode: Verwerking door elektriciteits- en gasleveranciers en door de onder hun verantwoordelijkheid handelende meetbedrijven van op Kleinverbruikers betrekking hebbende Persoonlijke Meetgegevens afkomstig uit Slimme Meters (Code of conduct: processing by electricity and gas suppliers and their suppliers of personal measurement data that originates from smartmeters of retail consumers) (Gedragscode Leveranciers Slimme Meters 2012)**

| *Domain* | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
|---|---|---|---|---|---|---|---|
| **Effectiveness** | 0 | 0 | 0 | 5 | 0 | 5 | |
| **Strictness** | 0 | 0 | 0 | 5 | 0 | 5 | |
| **Practicability** | 0 | 0 | 0 | 5 | 0 | 5 | |
| **Sustainability** | 0 | 0 | 0 | 4 | 0 | 4 | May need to be updated to reflect the new EU Privacy Directive by 2017/2018 |
| **Conflicting** | 0 | 0 | 0 | 1 | 0 | 1 | |

**#: 34 Title: Aanbeveling over na te leven beginselen bij smart grids en slimme meters [Recommendation]**

| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | *Explanation* |
|---|---|---|---|---|---|---|
| **Effectiveness** | 0 | 0 | 3 | 3 | 0 | Aims to protect the privacy of customers, but a customer is not a direct actor |
| **Strictness** | 0 | 0 | 3 | 3 | 0 | |
| **Practicability** | 0 | 0 | 0 | 0 | 0 | |
| **Sustainability** | 0 | 0 | 2 | 2 | 2 | |
| **Conflicting** | 0 | 0 | 3 | 3 | 3 | Not sure about conflicts; no analysis is done by the policy maker on this aspect who only looks to this from the policy aspects because it is a recommendation, not policy to be implemented 1-0-1 |

| **#: 35** | **Obligation to update the application and system software of smart meters in case the manufacturer requires that [5], art 26ac** |
|---|---|

| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | *Explanation* |
|---|---|---|---|---|---|---|
| **Effectiveness** | 0 | 0 | 5 | 5 | 5 | Not sure whether the DSO network operator operates a connection DER power flow measuring component; if so this applies to DER as well |
| **Strictness** | 0 | 0 | 5 | 5 | 0 | |
| **Practicability** | 0 | 0 | 4 | 4 | 4 | Practical issue when over the air (OTA) is not possible |
| **Sustainability** | 0 | 0 | 5 | 5 | 5 | |
| **Conflicting** | 0 | 0 | 1 | 1 | 1 | |

| **#: 40** | **Title: Law 24/2013 Spanish electricity sector regulation** |
|---|---|

| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | *Explanation* |
|---|---|---|---|---|---|---|
| **Effectiveness** | 4 | 5 | 5 | 5 | 5 | Objectives are clear |
| **Strictness** | 3 | 5 | 3 | 3 | 5 | Boundaries defined but measurable objectives are only defined in the Generation and Customer domains |
| **Practicability** | 5 | 5 | 5 | 5 | 5 | |
| **Sustainability** | 5 | 5 | 5 | 5 | 5 | |
| **Conflicting** | 1 | 1 | 1 | 1 | 3 | Customer requirements can come in conflict with European Regulation |

| **#: 41** | **Title: Royal Decree 1955 / 2000 of 1 December, which regulates the activities of transport, distribution, marketing, supply and installations of electricity authorization procedures. Last updated 1/704/2016** |
|---|---|

| *Domain* | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | ES & DH | *Explanation* |
|---|---|---|---|---|---|---|---|
| **Effectiveness** | 4 | 4 | 4 | 4 | 4 | 3 | Well defined |
| **Strictness** | 5 | 5 | 5 | 5 | 5 | 4 | There are well defined penalties in case of non-compliance. |
| **Practicability** | 5 | 5 | 5 | 5 | 5 | 4 | It is adopted by all stakeholders |
| **Sustainability** | 4 | 5 | 5 | 4 | 4 | 4 | End price of energy has complex calculation. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | No conflict is detected |

| **#: 42** | **Title: Law August 23, 2004, # 239 "reorganisation of the energy sector, as well as delegates to the Government to restructure the existing provisions on energy** |
|---|---|

| *Scope* | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | *ES & DH* | *Explanation* |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Effectiveness** | 5 | 4 | 2 | 1 | 1 | 4 | Distribution, DER and customer not included. |
| **Strictness** | 5 | 5 | 1 | 1 | 1 | 3 | Penalties are well defined. |
| **Practicability** | 5 | 5 | 1 | 1 | 1 | 3 | Different guidelines are available. |
| **Sustainability** | 5 | 5 | 1 | 1 | 1 | 4 | Implemented. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | None identified. |

| **#: 43 Title: LEGISLATIVE DECREE No 387 of 29 December 2003** | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Scope*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | ES & DH | *Explanation* |
| **Effectiveness** | 4 | 4 | 4 | 1 | 1 | 4 | Requirements defined. |
| **Strictness** | 5 | 5 | 5 | 1 | 1 | 5 | Obligations of stakeholders. |
| **Practicability** | 5 | 5 | 5 | 1 | 1 | 5 | It is mandatory for all stake-holders |
| **Sustainability** | 4 | 5 | 5 | 1 | 1 | 5 | Customers' requirements are not well defined. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | No conflict is detected |

| **#: 44 Title: France • Article 7 which implement directive 2012/27/EU** | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | ES & DH | *Explanation* |
| **Effectiveness** | 3 | 3 | 3 | 3 | 1 | 3 | Many implementation issues need to be solved. It is still difficult to make a business out of energy efficiency. |
| **Strictness** | 2 | 2 | 2 | 2 | 1 | 2 | All Member States, apart from Sweden, have excluded energy use from the transport sector and 14 Member States have excluded their own energy use from the baseline used for target setting |
| **Practicability** | 3 | 3 | 3 | 3 | 3 | 3 | Stakeholders saw the need for the |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | European Commission to provide additional support to Member States through platforms (formal and informal) for the exchange of information, guidance materials or technical assistance. |
| **Sustainability** | 2 | 2 | 2 | 2 | 1 | 2 | Almost all stakeholders have identified consumer information as an essential element for the success of both EEOS and Alternative Measures. Most stakeholders felt that not enough resources are dedicated to this. |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | Factors for failure: lack of political will; lack of government capacity; lack of support instruments for obligated parties; lack of compliance mechanisms; high complexity; lack of suitable monitoring mechanisms |

| **#: 45** | **Title: Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC Text with EEA relevance** | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | ES & DH | *Explanation* |
| **Effectiveness** | 4 | 4 | 4 | 4 | 1 | 4 | There are different options for implementing Energy Efficiency Directive 2012/27/EU |
| **Strictness** | 5 | 5 | 5 | 5 | 1 | 5 | Mandatory in EU. |
| **Practicability** | 3 | 3 | 3 | 3 | 3 | 3 | It is necessary to evaluate at a National level the different options to be implemented. |
| **Sustainability** | 4 | 4 | 4 | 4 | 1 | 4 | There is a transition period |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | None identified. |

| #: 50 Title: Energy Independence and Security Act, VS, Section 1301 (2007) | | | | | | |
|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 0 | 5 | 5 | 5 | 0 | |
| **Strictness** | 0 | 3 | 3 | 3 | 0 | |
| **Practicability** | 0 | 4 | 4 | 4 | 0 | Costs only in a generic sense |
| **Sustainability** | 0 | 3 | 3 | 3 | 0 | Long-term vision; wording of (5) is however out of bounds |
| **Conflicting** | 0 | 3 | 3 | 3 | 0 | |
| Base framework for smart grid experiments and drive to move forward in a controlled fashion. | | | | | | |

| #: 51 Title: Roadmap Smart Grids (English Version), Netbeheer Nederland | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 3 | 3 | 3 | 3 | 3 | 0 | Roadmap – ESCO aspect in R&E |
| **Strictness** | 3 | 3 | 3 | 3 | 3 | 0 | Roadmap – ESCO aspect in R&E |
| **Practicability** | 3 | 3 | 3 | 3 | 3 | 0 | Roadmap – ESCO aspect in R&E |
| **Sustainability** | 0 | 0 | 0 | 0 | 0 | 0 | Roadmap will be adapted on the run to 2050 |
| **Conflicting** | 0 | 0 | 0 | 0 | 0 | 0 | |

| #: 52 Title: Smart Grid Strategy: The intelligent energy system of the future | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Domain*** | *Generation* | *Transmission* | *Distribution* | ES & DH | *DER* | *Customer* | *Explanation* |
| **Effectiveness** | 3 | 3 | 3 | 3 | 3 | 3 | Covers full sector including Heat Exchange |
| **Strictness** | 3 | 3 | 3 | 3 | 3 | 3 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Practicability** | 0 | 0 | 0 | 0 | 5 | 5 | |
| **Sustainability** | 4 | 4 | 4 | 4 | 4 | 4 | |
| **Conflicting** | 1 | 1 | 1 | 1 | 1 | 1 | |

Denmark uses smart grids since 2010. There is an Energy agreement that at least 50% of the power generation is wind power produced by 2020. 35 smart grid recommendations were submitted in Autumn 2011.

- Remote hourly metering by 2016
- Flexible energy consumption
- Nothing on privacy

CYBER SECURITY: Control of flexible consumption will entail a need for increased automation, remote control, and exchange of data with other IT systems. Ultimately it will also entail new security-related challenges for the electricity system as a whole. Risks and possibilities of attacks on the electricity system as a critical infrastructure, as well as risks of misuse and distortion of data will increase and the traditional understanding of security in the electricity system therefore has to be expanded, with extra focus on cyber-attack threats and IT security and their associated risks, vulnerabilities and implications.

Smart grid is included in emergency management work in the energy area. This applies in particular to protection against cyber attacks and managing such attacks to reduce their effects on society. As responsible authority in the energy area, the Danish Energy Agency has the overall responsibility for emergency management and preparedness in the energy area, while Energinet.dk manages coordination of relevant enterprises and their emergency preparedness

To develop a software application which, via the Data hub, can give third parties secure, delegated access to data, with the consent of the user, in order to develop services in the energy area. Furthermore, the Data hub can be utilised to deliver aggregated data void of personal information. In December 2012, the Danish Safety Technology Authority, which is the authority responsible for electricity and metering security, published an analysis of the security-related challenges identified in connection with the smart grid

# Annex B: Various types of documents and their key characteristics

| | Binding / non-binding | Scope | Into force date | Deadline for application/ conversion |
|---|---|---|---|---|
| **(international) Convention** | Binding (sometimes with options) | Nations which signed the treaty | After ratification (by a defined number of nations) | No (apart from moral obligation) |
| **EU Strategy** | Self-binding | All EU bodies, institutions and/or EU MS and/or Int'l community | Date of publication | N/A |
| **EU Regulation** | Binding | All EU MS | Defined in publication | Yes |
| **EU Directive** | Binding | All (or specific[4]) EU MS | Defined in publication | Yes |
| **EU Decision** | Binding | Specific MS, body or organisations | Defined in publication | Yes |
| **Recommendation (by EU institution/body)** | Non-binding | To be specified | N/A | N/A |
| **Opinion (by EU institution/body)** | Non-binding | To be specified | N/A | N/A |
| **Norm** | Self-binding, may be mandated by law | Energy sector / SG domain / manufacturer | Publication date | N/A |
| **Standard** | Self-binding | Energy sector / SG domain / manufacturer | Publication date | N/A |
| **Code of Conduct** | Voluntary self-binding | Energy sector / SG domain | Publication date or into force date | N/A |
| **Good Practice** | May be voluntary self-binding | Energy sector / SG domain | N/A | N/A |
| **Recommendation** | Non-binding | Energy sector / SG domain | N/A | N/A |
| **Guideline** | Non-binding | Energy sector / SG domain / related organisations | N/A | N/A |

[4] In practice, EU Directives address all MS.

| | Binding / non-binding | Scope | Into force date | Deadline for application/ conversion |
|---|---|---|---|---|
| **National Strategy** | Self-binding | All of government, and/or public-private and/or public-private-academic and/or int'l community | Date of publication | N/A |
| **Legislative Act ('law')** | Binding | Nationwide or (critical) sector specific | Date of official publication or published date of entry into force | N/A |
| **Administrative Decree ('regulation')** | Binding | Nationwide or (critical) sector specific | Date of official publication or published date of entry into force | N/A |

# Annex C: Full list of considered documents

| # | Title |
|---|---|
| 1 | Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace |
| 2 | Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities |
| 3 | Directive 2002/20/EC of the European Parliament and of the Council on the authorisation of electronic communications networks and services |
| 4 | Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision |
| 5 | Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information se-curity across the Union |
| 6 | Directive 2002/22/EC of the European Parliament and of the Council on universal service and users' rights relating to electronic communications networks and services |
| 7 | Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector |
| 8 | Regulation (EC) No 1211 / 2009 of the European Parliament and of the Council establishing the body of European regulators for electronic communications (BEREC) and the Office |
| 9 | Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' |
| 10 | Smart Grids European Technology Platform (ETP Smart Grids) |
| 11 | ENISA - Communication Network Interdependencies in Smart Grids |
| 12 | CEER status review on European Regulatory Approaches Enabling Smart Grid solutions (Smart regulation) |
| 13 | Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Smart Grids: from innovation to deployment |
| 14 | Smart grid security certification in Europe: Challenges and recommendations |
| 15 | CEN-CENELEC-ETSI Smart Grid Coordination Group - Smart Grid Information Security |
| 16 | Directive 2008/114/EC on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection |
| 17 | Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" |
| 18 | Communication from the Commission on a European Programme for Critical Infrastructure Protection |
| 19 | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) |
| 20 | Smart grid policy in the United States |
| 21 | Smart Grid Interoperability Panel: Cybersecurity Information Sharing in Electric Utilities |
| 22 | Cyber Security Information Sharing Act |

| | |
|---|---|
| **23** | Regulation (EU) No 611/2013<br>of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications |
| **24** | ECHR - as underlying basis to e.g. privacy law and human rights |
| **25** | Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) |
| **26** | The Working Party on the protection of individuals with regard to the processing of personal data. This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. |
| **27** | Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA |
| **28** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)<br>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) |
| **29** | Opinion of the European Data Protection Supervisor (EDPS) on the Commission Recommendation on preparatioin for the roll-out of smart metering systems |
| **30** | Smart Grid issues in Law and regulation |
| **31** | Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) |
| **32** | Dutch law that allow consumers to OPT-OUT: refuse a smart meter's communication function |
| **33** | Gedragscode: Verwerking door elektriciteits- en gasleveranciers en door de onder hun verantwoordelijkheid handelende meetbedrijven van op Kleinverbruikers betrekking hebbende Persoonlijke Meetgegevens afkomstig uit Slimme Meters |
| **34** | Aanbeveling over na te leven beginselen bij smart grids en slimme meters (CO-AR-2011-004) [Recommendations about principles to be applied for smart meters and smart grids], Belgian Commission For Data Protection |
| **35** | Obligation to update the application and system software of smart meters in case the manufacturer requires that (Elektriciteitswet art 26ac) |
| **36** | various national laws & regulations |
| **37** | Smart Grid Pilots Part 1: Handvatten wet- en regelgeving intelligente netten |
| **38** | Belemmeringen van wet- en regelgeving voor smart grid diensten [Law and regulation barriers for smart grid services], Copernicus Inst., Univ. Utrecht |
| **39** | Smart Grid Pilots deel 2 Handvatten voor wet- en regelgeving [SG Pilots: relevant law and regulation], univ Amsterdam, Univ. Utrecht, TNO |

| | |
|---|---|
| **40** | Law 24/2103 on the electric sector |
| **41** | Royal Decree 1955/2000 |
| **42** | Riordino del settore energetico, nonche' delega al Governo per il riassetto delle disposizioni vigenti in materia di energia |
| **43** | Legislative Decree No 387 of 29 December 2003 |
| **44** | Article 7 which implement directive 2012/27/EU |
| **45** | Framework for improving Critical Infrastructure Cyber Security (NIST framework that focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.) |
| **46** | NISTIR 7628 Guidelines for Smart Grid Cyber Security - The three-volume report, NISTIR 7628, Guidelines for Smart Grid Cyber Security presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. |
| **47** | European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security |
| **48** | Critical information infrastructure protection: towards global cyber-security European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI)) |
| **49** | Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC Text with EEA relevance |
| **50** | Energy Independence and Security Act, VS, Section 1301 (2007) |
| **51** | Roadmap Smart Grids (English Version) |
| **52** | Title: Smart Grid Strategy: The intelligent energy system of the future |
| **53** | Wet gegevensverwerking en meldplicht cybersecurity |
| **54** | Nader rapport bij Wet gegevensverwerking en meldplicht cybersecurity |