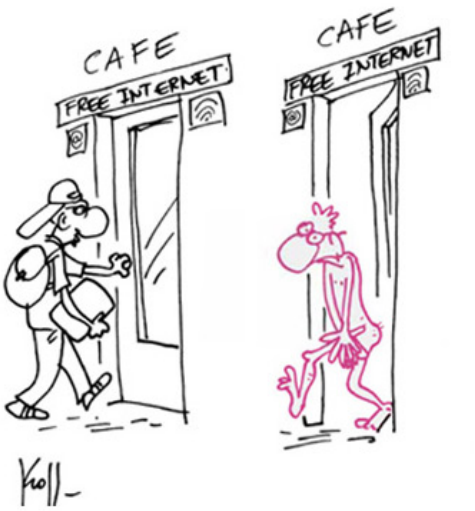
Winter February, 2013

Legal Protection by Design in the Smart Grid

Mireille Hildebrandt, *Radboud University Nijmegen*



LEGAL PROTECTION BY DESIGN IN THE SMART GRID

Privacy, data protection, profile transparency

Prof. dr. Mireille Hildebrandt

Chair of Smart Environments, Data Protection and the Rule of Law
Institute of Computing and Information Sciences (iCIS)
Privacy & Identity Lab
Radboud Universiteit Nijmegen

Assignment for the SmartEnergyCollective (SEC)
http://www.smartenergycollective.com/site/pagina.php?

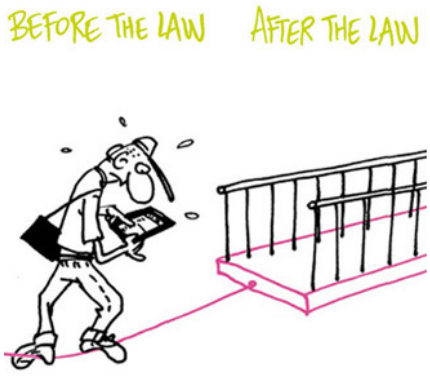
Preface

This study entails a reflection on the legal requirements for a level playing field on which all stakeholders in the future Smart Grid may pursue maximum value creation. It has been commissioned by the Smart Energy Collective, and aims to respond in a coherent way to the following set of questions:

- A summary of the present legal requirements that originate from the current European legislation [Chapter 2]
- What are potential design implications of the latitude for (national) implementation that the European directives allow? [Sections 3.4 and 4.4.1]
- What are potential design implications of the European Data Protection Regulation that has recently been proposed? [Chapter 2, further discussed in chapter 4]
- How should one interpret the increasing disconnect between the current geographically defined laws and regulations and social and economic developments that supersede the jurisdiction of the nation-state? [Sections 4.1.2; 4.4]
- What are relevant legal and social developments that might impact the design of smart energy systems which can be expected in the upcoming decades? [Chapters 1, 2]
- Does the number one security goal of availability for critical infrastructure systems impose (legal) restrictions on the use of data streams in smart energy systems? [Section 3.3]
- Should the creation of added value on data used for system optimization be allowed? [Sections 2.2.6; 2.2.7; 3.3; 4.1.4.1; 4.1.7]
- Should added value creation through ancillary energy services be based on a separate data stream? [Sections 2.2.6; 2.2.7; 3.3; 4.1.4.1; 4.1.7]
- Do the costs associated with investment in security expertise to prevent substantial privacy breaches drown out the supposed benefits? [Sections 3.3; 4.1.10.1; 4.1.10.2]

The challenges formulated in these questions relate to two notions that are fundamental for a sustainable ICT infrastructures such as the Smart Grid:

1. Intuitive transparency with regard to the potential consequences of sharing one's data.
2. Default hardwired contextual integrity that does not put the burden of protecting against undesired profiling on the shoulder of individual consumers.



Introduction[1]

As indicated in the preface this study entails a reflection on the legal requirements for a level playing field on which all stakeholders may pursue maximum value creation using smart energy services in a smart grid environment. A serious roll-out of the Smart Grid will require various types of predictive modelling to achieve a more balanced management of resources, notably when the system should enable demand response, decentralization of energy supply, the growth of a new type of 'prosumers', the institution of local markets for energy exchange, and the integration of various types of renewable energy (e.g. solar and wind). The challenges faced by the introduction of a new system for energy generation, distribution, transport and exchange reside in safeguarding its resilience in the face of natural disasters, malicious attacks, market disruptions and system breakdowns. On top of that the usage of advanced data analytics to achieve load balancing, desirable pricing incentives as well as resilience may impact human rights and civil liberties such as privacy and data protection, especially the right to profile transparency.

Next to these major challenges so-called Energy Service Companies (ESCOs), seen as third parties with regard to energy supply and demand,[2] will create value added services that should incentivize end-users to reorganize their energy consumption in a way that (1) reduces their energy requirements, (2) reduces $C0_2$ emissions, (3) enhances the network's resilience, and if possible, (4) enables them to generate renewable energy to be fed back to the net. These value added service will often require access to Big Data, thus enabling reliable predictive user modelling, which poses new threats to privacy & data protection, non-discrimination and due process.

The focus of this study will therefore be on the implications of data analytics and profiling rather than merely on the storage of personal data. We note that the introduction of the smart meter has already provided for numerous studies of its impact on the privacy and data-protection of end-consumers. In the Netherlands this has led to the statutory right to refuse the

installation of a smart meter, or – for those with a smart meter - the right to refuse to have personal data sent to the network operator. The question in this study will not be whether smart meters violate the privacy of individual users, but:

> Which should be the requirements for the complex network of machine-to-machine interactions within the Smart Grid so as to prevent illegitimate and unlawful violations of privacy law and data protection legislation?

Such requirements are preconditions for a trustworthy infrastructure capable of resisting dangerous fluctuations in the level of trust that is needed for a smooth operation of the infrastructure. Referring to the financial crisis it should be clear that linking a Smart Grid to potentially volatile financial markets can easily undermine consumer trust and stifle innovation. The same goes for a Smart Grid that comes to depend on business models that trade personal data and personalized profiles based on anonymized data. Once consumers realize that they are being targeted in ways that cannot be foreseen, while these profiles will have a major influence on their life, they may refrain from endorsing the Smart Grid. This will frustrate the objectives set out in European legislation and those of various industry initiatives. The point is not to obstruct the vision of the Smart Grid but to investigate how it can model itself on the future requirements of Data Protection by Design and Default, as introduced in the draft General Data Protection Regulation of the European Union.

For this reason, an important sub-question will be:

> How is the right to profile-transparency articulated within the EU legal framework and how can this right be turned into an effective right without necessarily destroying business models based on value added services?

Finally, the notion of value added services requires an investigation into how energy end-users can become partners in the production of data and data derivatives instead of merely being a cognitive resource for the personal data economy run by short term commercial interests. This involves a second sub-question:

> How can energy consumers be involved in future business-models as data prosumers, sharing the benefits of advanced data analytics? Can we have our cakes and eat them too: enjoy the benefits of personalized services without losing all control over how we are being profiled?

Mireille Hildebrandt, Nijmegen 14th January 2013

Chair of Smart Environments, Data Protection and the Rule of Law
iCIS, Radboud University Nijmegen
PILab

Executive Summary

In chapter 1 the notions of the Smart Grid, Profiling technologies and Legal protection by design are discussed, refined and defined.

1. The Smart Grid is distinguished from the smart meter and explained from the perspective of the EU legal framework, since this will set the constraints that should enable the achievement of a Smart Grid infrastructure within the EU. The working definition highlights the visionary and ambitious nature of the idea of the Smart Grid, that is expected to enable distributed energy generation, the uploading of renewable energy by individual households, flexible pricing incentives, granular information on energy consumption of final users, remote reading and remote control for network operators, demand response and real-time load balancing. In chapter 3 the EU legal framework for energy efficiency, renewable energy in the EU internal market is further elaborated.
2. The notion of profiling technologies or data analytics is explained as conditional for many aspects of the Smart Grid as envisioned today. Profiling will determine the 'smartness' of the grid and and basically involves techniques of artificial intelligence, such as machine learning and other types of smart automation. Profiling will also inform the interventions of energy service companies that should offer value added services to customers are expected to contribute to energy savings.
3. Finally, the notion of legal protection by design (LPbD) is introduced and discussed, referring to the need to pay trained attention to potential infringements of fundamental rights by emerging technologies, notable by profiling technologies. LPbD insists that the legal requirements of fundamental rights such as privacy and data protection must be translated into computer system hardware, code, protocols and organisational standards to sustain the effectiveness of such right in a changing technological landscape.

Chapter 2 presents potential technical solutions that could help achieve legal protection by design in smart grids. This chapter is the follow-up of the legal analysis of chapter 4 that develops the legal requirements of the fundamental rights of data protection, privacy and non-discrimination with respect to the smart grid. It is presented up-front because it presents the outcome of the study in practical terms. In that sense this chapter forms the core of the report.

First, the legal requirements for the Smart Grid (as further elaborated in chapter 4), are discussed and matched with proposals for LPbD. These legal requirements are in no way exhaustive, but hope to mark the most salient outline of the complex system of rights and obligations for data processing in the context of the Smart Grid. This involves legal requirements of:

- Right to Universal Service
- Legal certainty and level playing field in the EU
- Energy usage behaviour as personal data
- Data Protection Impact Assessment
- Confidentiality & security by design
- Fair processing
- Consumer-driven added value services
- Sensitive data and non-discrimination
- Consent
- The right to be forgotten
- Data portability
- Measures based on profiling
- Liability of data controllers and processors

Second, a typology is developed of potential technical solutions, mapping various types of proposed solutions together to increase understanding of different strategies to safeguard privacy and data protection. While these strategies may overlap and often address similar problems, they thus provide a multilevel approach capable of preventing, resolving or balancing infringements of fundamental rights.[3] The types developed in this study are not meant to be exhaustive and depending on the context other listings could make more sense. The following 7 types are distinguished in relation to legal requirements for the Smart Grid:

1. Separation of data streams, end-2-end encryption and secure authentication
2. Personal data vaults or similar solutions
3. Privacy preserving data mining [PPDM] and aggregation techniques to achieve anonymisation
4. Management of credentials instead of identification
5. Metadata, semantic web and agreement technologies
6. Discrimination aware data mining [DADM]
7. User centric personal data ecosystems [PDE)

Chapter 2 ends with a set of general recommendations, that is repeated in the conclusions (see below).

Chapters 3 and 4 form the legal backbone of this study. They provide an overview of the relevant EU legal framework that enables and constrains the development of the Smart Grid. The legal requirements discussed in chapter 2 have been derived from these chapters, mostly from chapter 4.

Chapter 3 elaborates the EU legal framework for the energy market, starting with the right to universal service that underpins the legislative framework of the critical infrastructure. This chapter presents the objectives of energy efficiency, enery usage from renewable sources, the constraints of the internal energy market; the introduction of the smart meter; the need for and requirements of the Cost Benefit Analysis; and the margin of appreciation for the MSs.

Chapter 4 elaborates the EU legal framework of relevant fundamental rights with a clear focus on data protection legislation. In view of the proposed General Data Protection Regulation that is expected to come into force by 2016 at the latest the current and future law on data protection is discussed similtaneously as much as possible, detailing the more stringent approach of the Regulation in terms of enforcement, auditibility and liability.

Chapter 5 provides succinct answers to the research questions raised in the introduction, followed by the following set of general recommendations:

1. Think in terms of data flows instead of isolated discrete data; foresee whether de-anonymisation will reinstate identifiability and treat data streams that are susceptible to such de-anonymisation as falling within the scope of data protection legislation.
2. Make privacy and security an essential part of your business-model, do not treat them as costs but as a competitive advantage – especially in the long run.
3. Start from and reiterate Data Protection Impact Assessments.
4. Practice Data Protection by Design and by Default.
5. Develop software tools and hardware infrastructure that is innovative in terms of DPbDesign and by Default.
6. Develop business models based on DPbDesign and by Default.
7. Practice Security by Design, notably end-to-end encryption and secure authentication wherever possible.
8. Invest in recurrent software analyses.
9. Practice discrimination-aware data mining.
10. Base your trust management on trustworthiness.
11. Never underestimate the recurrent cost of safety and security.
12. Don't allow critical infrastructure to depend on volatile markets.
13. Create separate data streams for (1) critical infrastructure that protects the right to universal service, and (2) commercial value added services.
14. Design profile transparency in the back-end of the Smart Grid system.
15. Design intuitive interfaces that provide transparency about the potential consequences of sharing one's data (showing what profiles they match).
16. Design for profile transparency in the front-end of the Smart Grid system (allow consumers to play around with their data to figure out how they are matched).

Table of contents

1 DEFINING THE SMART GRID, PROFILING TECHNOLOGIES, LEGAL PROTECTION BY DESIGN

1.1 SMART GRID

As yet, the Smart Grid is a vision, and different stakeholders tend to come up with different objectives, definitions and conditions. Strict definitions are unwise at this stage, since it is still unclear how the Smart Grid will finally come to pass. In this study I will focus on the vision of the EU legislator which has defined the Smart Grid as follows:[4]

> 'smart grid' means an upgraded energy network to which two-way digital communication between the supplier and consumer, smart metering and monitoring and control systems have been added.

As a background we can note that the present energy infrastructure in the EU is found to be in need of revision, while the foreseen energy needs in ICT-enabled societies are expected to surge. At the same time the targets for the reduction of CO_2 emissions have to be met. The idea is that a combination of savings on energy consumption, generation of renewable energy, real time distribution on the basis of demand response and pricing strategies that incentivize to achieve load-balancing will do the job. These policies are deemed conditional for (1) meeting future energy demand, (2) less dependence on fossil fuels that must be imported from outside Europe, (3) reducing CO_2 emissions and (4) lowering the overall cost of energy consumption. At the same time the Smart Grid should (5) facilitate the Smart Home that allows for ubiquitous machine-to-machine communication between various devices within – and possibly without - the home, combining remote control, smart automation of home appliances, transparency and control for the user with energy saving. This is connected to the notion of domotica that foresees further integration of various types of robots into the home environment, and remote healthcare that allows people to stay home despite serious disabilities or old age.[5] Finally, the Smart Grid should (6) facilitate increasing use of electrical vehicles, maybe one day resulting in the smart car that combines traffic management, safe driving, energy savings and reduced pollution.[6]

The Smart Meter is the interface between consumers and the Smart Grid and basically the enabler of the two-way communication between individual end-users, the smart home, the smart car and the Smart Grid. As such the Smart Meter will determine who gets to see and handle what data or information and under what conditions. Its characteristics are the capacity for remote reading, remote control and the mentioned two-way communication.

A more detailed working definition of the Smart Grid, as conceptualised in the European legal framework, involves the following dimensions:

- Distributed energy generation by individual households, windmill parks, industry
- Integration of renewable energy sources that can be fed back into the GRID
- Granular pricing strategies that incentivize energy saving and load balancing
- Smart metering that provides for two-way communication between the end-user and the GRID
- Smart metering that provides end-users, network operators, suppliers and – possibly also - ESCOs with granular information on energy consumption of the end-user
- Smart metering that provides for remote reading and remote control for the network operator, suppliers and the end-user
- A move from supply-side energy markets to demand-response
- Real-time load-balancing based on real-time metering and predictive analytics

The advantage of acknowledging this as a working definition is that it stays within the legal framework that determines the constraints that restrict and enable the envisaged EU energy market.

1.2 PROFILING TECHNOLOGIES AND DATA DERIVATIVES

The Smart Grid is smart to the extent that it integrates data analytics. In theory, these analytics could be 'dumb' in the sense of not being leveraged by machine learning techniques, merely providing precise data on energy usage.[7] It is, however, difficult to imagine that the enormous mass of data would mean anything to anybody if not mined for relevant patterns and explained by means of e.g. visual analytics, to provide information instead of mere data (which easily turns into noise). This is especially relevant in the case of load balancing (achieving optimal energy availability without costly storage for peak consumption) and flexible pricing strategies that should incentivize energy savings (based on short term and long term demand response).

Profiling technologies are based on data analytics. They entail two types of profiling that feed on each other.

- First, they allow for the *construction* of relevant profiles out of massive amounts of data. This process is often called knowledge discovery in databases (KDD); it seeks to mine non-obvious patterns in databases which allow for the construction of new insights that could not have been deducted or induced with the naked human eye. The inferences derived from big data can be coined as data derivatives.[8]
- Second, profiling technologies allow for the *application* of profiles to new data, often to predict certain behaviours. As such, these data derivatives can be monetized and traded, just like their financial namesakes.

The application of profiles mined on the basis of smart data analytics can be used as a recurrent if not permanent and real-time test of the construction of the profiles. This allows a continuous process of refinement and adaptation, for instance in response to changed circumstances. This functionality implies the learning capacity of profiling technologies and demonstrates that its artificial intelligence (AI) cannot be compared to that of the '80s of the last century (top-down context-insensitive good old fashioned artificial intelligence: GOFAI). Machine learning is generally defined as the capacity of machines to improve their performance based on feedback. In that sense we must define profiling technologies as part of the modern approach of artificial intelligence (AIMA).[9] It is closely related to and preconditional for proactive, adaptive and autonomic computing.

In relation to the Smart Grid profiling technologies are relevant at two levels. First, they are part of the 'smartness' of the grid, they allow for the data collected by automated remote readers to be used for demand response, load balancing, pricing strategies and for safeguarding energy availability as well as the various levels of security within the grid. Profiling technologies are – obviously – meant to enhance the reliability and versatility of the grid. However, one can imagine that some of the inherent unpredictability of e.g. machine learning creates fascinating risks for the critical infrastructure. This relates to security, energy availability, safety and overall costs. But is also relates to vulnerabilities related to the creation of added value based on data mined from the grid. This refers to the second level of relevance of profiling for the Smart Grid. Profiling technologies are part and parcel of the energy services to be provided by ESCOs. For instance, Nest Labs in the US develops a smart thermostat that helps end-user energy saving behaviour:[10]

> by studying its owner's habits and predicting things about when people are home and what they are likely to do with their home heating and cooling. (…) The device also collects enough data that Nest can start to draw from really large data sets on consumption and correlate that knowledge with information from other sources, like weather forecasts, to make a more powerful product. (…) Tony Fadell, Nest's founder and chief executive. "We can gather all that data, mix it with other data we store in the cloud, and push different algorithms to different houses to see how people react". That approach, continually testing one feature against another and going with the one that consumers responds to best, is called A/B testing when done with Internet software. It is how Google and others make their products. As more physical objects fill up with software and develop two-way interactions with the network, Mr. Fadell says, they can be developed the same way.

This rather extensive quote should sensitize us to the rather optimistic expectations based on the mining of Big Data and should warn us against a number of risks and uncertainties that could develop from careless experimentation with consumer energy consumption behaviour. If at any point consumers suspect that their behaviours are used to manipulate them, they may lose faith. Moreover, it may be that foreign intelligence services decide to take a look at such data, which may be less complex if they are stored in clouds with mandatory backdoors or failing security.[11] If such spying becomes known, consumers may again lose faith. Trust may plummet and to the extent that added value services draw their data from the critical infrastructure this may cause havoc for the Smart Grid.

Acknowledging that profiling technologies entail AI is important for three reasons:

1. They will enable the required automated responses that should make the future Grid Smart.
2. They will have a major influence on the vulnerability of the Smart Grid, due to safety and security risks generated by the inherent unpredictability of their automation
3. They will have a profound impact on privacy, data protection, non-discrimination and due process, further intensified in the case of trading with data derivatives

1.3 LEGAL PROTECTION BY DESIGN

The information and communication technology (ICT) infrastructure co-determines the bandwidth of social intercourse and determines how we perceive and cognize the world outside our immediate surroundings. Writing, the printing press and mass media have their own specific affordances as to how we perceive, understand and control our environment. The legal framework depends on the ICT infrastructure to orient, allow, prohibit or prescribe our interactions. Written law provides a particular type of legal certainty, based on written sources of law that provide a relatively stable staple of authoritative texts (codes, treaties, case-law, doctrinal treatises). This has created a need for interpretation, which delays and refines the judgment that decides the meaning of written codes. One could see this requirement of interpretation as an example of the transportation and distribution of meaning.

Interestingly the availability of relatively stable resources and the delays of transportation and distribution are not only core to the modern legal system that is based on written, enacted codes and authoritative, written judgments. They also define the 20th century notion of energy providing infrastructure: energy is kept in store to meet future needs; transport and distribution are defined by the delays inherent in supply side economics. With the advance of smart interconnected ICT infrastructures such as the Internet, the World Wide Web and its numerous applications, complemented with mobile and wireless communication networks we

can detect a shift from an infrastructure based on delays and stabilized resources towards a real-time and reduced-stock infrastructure. Whether this development is good or bad is not the topic of this study. Whether it is feasible and will indeed lead to reduced-stock energy management is another question, also not part of this study.

The law, however, needs to anticipate how these changes may affect its basic premises. The idea that written legal norms can coordinate the implicit affordances of smart infrastructures seems inadequate; the only way to ensure the sustainability of fundamental rights and liberties is to inscribe or design them into the architecture of the infrastructure. Unless we invent, engineer and design the smart grid in a way that meets the legal requirements of privacy and data protection, the Grid may simply collect and trade our energy consumption data with whoever pays best. Unless we invent, engineer and design the Smart Grid in a way that meets the legal requirements of non-discrimination and due process the Grid may enable insurance companies, law enforcement agencies, potential employers or credit brokers to discriminate us on the basis of an inferred pregnancy, religious affiliation, tax-evasion-behaviours or credit risk. The problem may either be that it allows for invisible unlawful discrimination, or it may be that lawful discrimination goes undetected. In both cases we have no idea of the profiles that match our data and therefore we have no idea how to change or hide behaviour to prevent undesirable discrimination. Our inferred preferences can be manipulated if we don't know that or how we have been profiled: we cannot defend ourselves against incorrect inferences and we cannot learn how our energy consumption behaviours impact the way we are treated. To remedy this situation certain requirements must be built into the infrastructure, re-creating an environment that fosters individual autonomy, treats us as worthy of equal concern and respect and provides intuitive transparency about the consequences of our interactions with the Smart Grid.

These requirements are not only ethical obligations for those investing in the Smart Grid. They refer to the Fair Information Principles (FIPs) that have been codified as law in many jurisdictions, notably in the EU Data Protection framework which will be discussed in the next section. The imperative that legal protection should be built into the ICT infrastructure has been termed legal protection by design.[12] We can define this as:

- Paying trained attention to the potential infringements of fundamental rights by emerging technologies, such as profiling technologies
- Taking note of the risks inherent in trading with data derivatives
- Developing legal requirements that fit the architecture and design of novel technological infrastructures, such as the Smart Grid
- Translating these legal requirements into computer system hardware, code, protocols and organisational standards
- Engaging lawyers, computer engineers, software developers and designers of human machine interfaces in the process of constructing new technologies and infrastructures
- Taking the protection of fundamental rights and the checks and balances of democracy and the Rule of Law as a basic premise and goal of the whole enterprise
- Thus levelling the playing field for the industry and other stakeholders to create added value based on business models that integrate the protection of fundamental rights into their core business

2 LEGAL PROTECTION BY DESIGN IN THE SMART GRID

2.1 LEGAL REQUIREMENTS, WITH PROPOSALS FOR 'LEGAL PROTECTION BY DESIGN'

This Chapter provides a set of proposals for legal protection by design. In this section the proposals are mapped according to the legal norms they may help to articulate. For an elaboration of the legal framework see chapter 3 (EU Energy Market) and especially chapter 4 (Fundamental Rights Protection).

Each heading refers to a legal right or obligation, formulated in terms of legal requirements for the Smart Grid and/or relevant stakeholders. The requirements are based on the current and the proposed upcoming legal framework, for explanation see the section to which the headings refer.

If possible, these requirements are then translated into proposals for legal protection by design. These proposals are not meant as exhaustive and are not necessarily compulsory.

2.1.1 Right to Universal Service (section 3.1.1)

1. Everyone has the right to access energy services. This imposes obligations on service providers to offer defined energy services under specified conditions, notably complete territorial coverage and affordable pricing.

2.1.2 Legal certainty and level playing field in the EU (section 4.1.2)

1. The introduction of a General Data Protection Regulation with direct legal effect in all the Member States entails that for all companies operating in the EU it becomes profitable to develop standards that articulate default compliance with EU data protection rights and obligations, since the legal requirements will be uniform across the EU.
2. All the legal rights and obligations stipulated in the proposed Regulation must be implemented by means of appropriate technical and organisational measures and procedures. The appropriateness will depend on the state of the art and the costs of implementation: technical and economic feasibility will determine the extent of a data controller's obligations.
3. Any business that wishes to engage with data processing of EU citizens will have to comply with EU data protection by design. The risk of effective liability, high fines and reputation damage will enforce a level playing field that will have a substantial impact on the standards of data protection worldwide.

2.1.3 Energy usage behaviour as personal data (section 4.1.3)

1. In the context of the Smart Grid all data on energy consumption should best be treated as personal data, taking into account that data aggregation or other techniques for anonymisation can reduce but not eradicate the risk of de-anonymisation.

2. This means that for all data streams containing energy usage data a Data Protection Impact Assessment will be required (see below) and Data Protection by Design and by Default (see below) must be implemented.
3. Note that in this view aggregation or anonymisation techniques can be viable implementations of DPbDefault, but do not render Data Protection legislation inapplicable.

2.1.4 Legal requirement of a Data Protection Impact Assessment (DPIA) (section 4.1.10.1)

1. Smart Grid initiators should not await the Commission's template but actively foresee the kind of impact the Grid may have on data protection rights and obligations.
2. They should envisage how alternative designs impact e.g.:
   a. data minimisation;
   b. meaningful consent;
   c. data portability;
   d. the right to forget;
   e. profile transpanency.
3. Various types of user participation should be organised, and the ability of users to understand the implications of their choices as well as their monitored behaviour should be ensured.
4. Designs that allow for high frequency trading with energy consumption behaviours (and the inferred data derivatives) must be avoided or at least separated from the data streams of the critical infrastructure since they will not empower the end-user and may cause volatility and unpredictable disruption of energy supply.

2.1.5 Legal requirements of confidentiality & security by design (section 4.1.10.2)

1. Security by Design seems to be a prerequisite for a resilient infrastructure, since the cost of security breaches and ensuing system breakdowns would be exponential.

   Proposals for Data Protection by Design
   a. End-to-end encryption seems indeed imperative. It is unclear to me why this is not mandatory law.
   b. Especially in the case of remote readings and wireless machine-to-machine communication between the Smart Grid and domotica, many security incidents can be prevented by imposing end-to-end encryption.
   c. The economics of security warrant a separation of the data stream of the critical infrastructure from that of value added services.

2.1.6 Legal requirements for fair processing (section 4.1.4 and 4.1.5)

1. In the context of the Smart Grid it would be advisable to separate data streams based on necessity (contract, legal obligation, vital interests of the user, public interest, legitimate interests of the controller) from those based on consent.

2. Since consent can be withdrawn at any time, it does not provide for a stable data stream; fluctuating trust levels around value added services could endanger the reliability of the Smart Grid or the availability of energy - if data streams are not separated.
3. Note should be taken that data streams based on consent must still comply with the conditions of data minimisation (i.e. purpose specification and use limitation, accuracy and completeness, and deletion or anonymisation as soon as the purpose is no longer relevant).

Proposals for Data Protection by Design and by Default:

a. It may save trouble to provide metadata for each data with the ground on which its processing is based, code for the purpose of processing and for the type of recipient of the data. This could make it easier to comply with transparency and auditability obligations and could fit with software that allows end-users to access their data in a format that easily sorts different types of data in a handsome overview.
b. To the extent that such metadata function as sticky policies that determine how they can be shared and used, they could implement data minimisation and fulfil the requirements of data minimisation. They could thus enable what the proposed Regulation means with 'Data protection by default'.
c. Special care should be taken to prevent that metadata generate more or more serious data protection vulnerabilities than they aim to solve.
d. Another option would be to put data in a personal data closet with an intelligent agent that checks, records, remembers, calculates which data are with whom/what on what grounds, for what purpose, and which types of third parties may assess them.
e. In the contexts of the Smart Grid DPbDefault entails very strict default settings for the data stream of the critical infrastructure itself, preferably hardwired into the architecture.
f. At the same time it should provide similar – softwired - technical protection for data streams that nourish the applications of ESCOs, requiring them to clarify on the basis of machine-to-machine communication what data they need for what purpose, providing transparency for any secondary use (such as selling the data or data derivatives). This can be achieved by use of meta-data with sticky policies and/or agreement technologies.
g. This could be combined with a software tool that allows only credentials for value-added services, e.g. integrated with a personal data vault, and an intelligent agent (agreement technologies).

2.1.7 Legal requirements for consumer-driven added value services (section 4.1.5)

1. In an environment where unexpected patterns may incentivize new business models and create unforeseen added value, data minimisation could stifle innovation.

Proposals for Data Protection by Design:

a. One solution for this problem would be to engage users, allowing their participation – based on enhanced transparency, open source software and intuitive interfaces that show what is done with their data and how matching profiles might impact them.
b. This will turn energy prosumers into data and profile prosumers, taking serious their participation in the creation of added value.

c. Profile-transparency, the right to forget and data portability are preconditional for such participation.
d. Taken together this will amount to a user centric personal data ecosystem approach.

2.1.8 Legal requirements in relation to sensitive data and non-discrimination (section 4.1.6)

1. Profiling enables 'masking' [prohibited discrimination on the basis of trivial – non-sensitive – data that correlate with sensitive data].

Proposals for Data Protection by Design:

a. To protect against masking discrimination-aware data mining may be required.
b. Alternatively, an intelligent agent may be developed that can inference such correlations, and check via feedback loops and P2P communications with other agents whether such discrimination is indeed at stake.

2.1.9 Legal requirements of consent (section 4.1.7)

1. Under the proposed GDPR the burden of proof that consent has been given is with the controller, and consent can be withdrawn any time.
2. A person should only give consent for the application of profiles if she is provided with the required transparency.

Proposals for Data Protection by Design:

a. All services for which consent is required should be switched off by default.
b. The consent switch should be granular enough to invite deliberate decisions but not overestimate the attention span of individual users:
   - the switch must be easy to use for withdrawal of consent;
   - on the basis of metadata built-in alarm signals should notify users of data and policy breaches and easy to understand notifications of changes in relevant policies or protocols, allowing for smart usage of the switch;
   - different switches could be designed for data used to *construct* profiles and those used to *match* a person with existing profiles.

2.1.10 Legal requirement of the right to be forgotten (section 4.1.8.1)

1. The proposed Regulation requires mechanisms to have personal data erased, this means that the architecture should entail DPbDefault: automated deletion as soon as data minimisation requires it.
2. The proposed Regulation requires mechanisms to facilitate easy access of data subjects to their data, and easy implementation of their right to have data deleted in case of withdrawal of consent or unlawful processing.
3. The proposed Regulation requires mechanisms to erase data after having provided them in function of data portability.
4. The term 'mechanism' is not defined in the Regulation but should be understood in a broad sense, it seems to refer to a mix of automated or semi-automated procedures, protocols, standards, certifications, software tools that generate a default setting for specific operations.

Proposals for data protection by design and default

a. In the case of the right to be forgotten, mechanisms should enable sophisticated, flexible consent management, e.g. by means of visualisation techniques, or sticky policies (with time stamps) combined with theorem provers.
b. The to-be-deleted data that reside with third parties must be targeted to make the right effective, implying the use of e.g. the Semantic Web to chase one's data across the web.

2.1.11 Legal requirement of data portability (section 4.1.8.2)

1. Data portability means that a data subject can obtain her energy usage data from the DNO and/or supplier, or from the ESCO that was processing them.
2. The data must be provided in an electronic and structured format, e.g. via a secure online environment, or on a disc, or the data could be transferred straightaway to the new supplier or ESCO, or even deposited in a personal data vault.
3. Since the DNO is the party that transfers relevant data to the suppliers or to the ESCO, it is not clear what data portability could mean in relation to the DNO. Should we foresee a time when DNOs are in competition across MSs?
4. The system may be designed in a way that keeps the data in a personal data vault, giving the data subject control over who gets to access the data. In that case portability is not the issue, but the right to be forgotten by the previous supplier or ESCO remains pertinent.

2.1.12 Legal requirements for measures based on profiling (section 4.1.8.3)

1. Measures based solely on automated profiling are prohibited, except in the case of a legal obligation, a contract or consent.
2. Profiling on the basis of energy usage data can be based on a legal obligation (e.g. national legislation that stipulates the roll-out of smart meters and load balancing).
3. It can also be based on the contract with the energy supplier or with an ESCO (they may even be the same company) or on consent.
4. *If allowed on one of these grounds* the consumer must be provided with information about the fact that measures are taken based on automated profiling and they must be provided with information about the envisaged effects. This can be summarized as profile transparency.
5. We can discriminate between back-end, front-end en interface transparency.

Proposals for data protection by design:

a. Profile transparency must be realised in the back-end system, rendering the lawfullness of the data mining operations auditable – while taking into account trade secrets and intellectual property rights.
b. Profile transparency must be realised by means of attractive interfaces that allow users to access information about the way they are profiled and how this may impact them.
c. Profile transparency must be realised in the front-end of the system, inviting users to interact with their profiles, understanding how their energy usage behaviour is interpreted by the profiling technologies.
d. Another possibility is to put data in a personal data closet with an intelligent agent (inference machine) that mines own data and those of peers and thus:
    a. what profiles a user matches.
    b. e.g. advices to withdraw consent and/or to order erasure.

2.1.13 Liability of data controllers and data processors (section 4.1.12)

1. In terms of the law the question is *not* whether a company or a public body designates itself as either a controller or a processor. This will be established on the basis of *actual control and delegation*.
2. Under the proposed Regulation fines of up to 1.000.000 euro or 2% of the annual worldwide turnover are possible (competition law types of penalties).
3. The liability of controllers and processors of personal data under the proposed GDPR will require the articulation of all mandatory rights and obligations of the data protection framework into the Smart Grid architecture.
4. Combined with
    a. the imposition of DPbDefault (data minimisation),
    b. DPbDesign (early uptake of all the relevant rules and principles in the architecture)
    c. the introduction of new rights such as data portability, and
    d. newly articulated rights such as the right to be forgotten and
    e. rights against unwarranted profiling

the imposition of liability will force the industry to innovate on the basis of a level playing field.

5. Techniques, technologies, applications, hardware, code, software and protocols will be invented and/or reinvented to make data protection part and parcel of the business model of advanced smart environments.
6. The development of the Smart Grid will benefit from early investment into security and privacy by design, preventing rising costs of ICT maintenance and preventing dangerous fluctuations in consumer trust. Those who fail to comply will be out of business.

2.1.14 Cookie legislation and data retention obligations (section 4.2)

1. If energy usage behaviour data are transmitted by means of a publicly available communication service or network:
    a. tracking mechanisms such as cookies require informed prior consent;
    b. traffic data must be retained in accordance with the national law that implements the Data Retention Directive; such data must be accessible for law enforcement under strict conditions in specific cases.

2.1.15 Police and Criminal Justice (section 4.3)

1. Smart grid operators should foresee that, especially in the context of fraud detection or tax evasion, law enforcement may seek ways to access energy usage data. This may concern either the usage data of a specific person, who is already under suspicion or Big Data that allow to create data derivatives deemed to aid criminal intelligence.
2. To the extent possible the architecture should prevent and rule out easy access to large amounts of energy usage data as this would be contrary to the principle of purpose binding. In individual cases and under strict legal conditions access should be enabled and it would help if the architecture has a default setting against easy access.

3. This is especially urgent for either specific personal data or Big Data collected by third parties who may be tempted to provide such specific or aggregated, anonymised data on a voluntory basis. Though this would obviously violate the legal requirements of data minimisation (purpose limitation, prohibition of secondary use without explicit consent), it may be difficult to audit such violations after the data have been anonymised.

2.1.16 Cloud Computing (section 4.4)

1. Smart Grid operations that concern critical infrastructure should not be managed in public clouds for reason of energy availability, grid resilience and other security, privacy and data protection concerns.
2. Smart Grid applications that concern added value services should not be run in public clouds because of increased data protection risks.
3. To the extent that private clouds could provide benefits in terms of security, privacy and data protection, decisions on their employment and the relevant conditions should be part of the DPIA.

2.2 TYPOLOGY OF POTENTIAL TECHNICAL SOLUTIONS

In this section the technical articulation of proposals for legal protection by design are categorised: (1) separation of data streams, end-2-end encryption and secure authentication (2) data vaults, (3) privacy preserving data mining & aggregation techniques, (4) credentials management instead of identification, (5) metadata, semantic web & agreement technologies, (6) discrimination aware data mining, (7) user centric personal data eco system.

Some of these potential solutions address privacy and security in the sense of confidentiality and access control, some articulate data minimisation, others provide tools that should empower energy consumers to play around with their data and become a partner in the business model of value added services. Though we can expect that the types of solutions can and will be combined, this is not always possible. Choices will have to be made, taking into account that some solutions are path-dependent, making it more difficult to opt for other solutions at a later point in time. The famous Dutch proverb stating that sometimes we must spend a dime to earn a pound is relevant here: architecture is politics and wise anticipation can prevent a host of foreseeable problems.

2.2.1 Separation of data streams, end-2-end encryption and secure authentication

The most simple solutions to some of the problems that can be foreseen when massive amounts of energy usage data are processed are: (1) to separate the datastreams that nourish the critical infrastructure from those that nourish advertising, marketing and law enforcement; (2) end-2-end encryption wherever data are transferred between devices, meters, network operators, suppliers and ESCOs and (3) secure authentication to control access to the data. The first concerns the articulation of the purpose limitation into the architecture of the Smart Grid, the second concerns the confidentiality of energy usage data en the third concerns control over the access to the same data.

One caveat may be that separating data streams may lead to sound protection for the critical infrastructure but unintentionally allow sloppy protection for privacy and data protection. It is important to emphasize that data processing on the basis of a contract or consent still requires compliance with e.g. purpose limitation. Another caveat concerns the question of how separation of data streams relates to local, distributed data streams that allow for local energy markets with flexible pricing strategies and local demand-response.

2.2.2 Personal Data Vaults or similar solutions

The idea would be to keep energy usage data in a personal data vault with strict protocols that determine who gets to access what data for how long, for what purpose, to be shared with what other entity etc. This should also provide accurate data on who accessed what data for what purpose on what legal ground etc. The vaults can be kept on the hardware of the user or with the provider of the virtual vaults (centralized or distributed);[13] these are important choices, relating to security and privacy issues. Profiling can still be done, but in some systems it seems that cross-contextual profiling and aggregate profiling is no longer possible. This depends on architectural choices. Google autocomplete (and page rank) would work very differently if based only on the data of one's own previous searches.

This type of solution could provide compliance with data minimisation and could empower users as data & data derivative prosumers, depending on the functionality of the protocols that hold the system together.[14] It can be integrated with the other solutions.

2.2.3 Privacy preserving data mining (PPDM) and aggregation techniques to achieve anonymisation

In relation to data mining and profiling software has been developed that enables analytics with a minimal or no disclosure of personal data, called privacy preserving data mining (PPDM).[15] This could be implemented on the side of network operators, energy suppliers as well as energy service companies whenever they need to perform analytics on data aggregates. This way data minimisation can be accomplished, while various types of profiling are made possible.[16]

2.2.4 Management of credentials instead of identification

This concerns authentication and authorisation based on attributes or credentials instead of full identification.[17] This is a straightforward application of data minimisation. Profiling becomes a different thing or impossible, depending on whether and what data are linkable.

For the Smart Grid this could be interesting whenever the sharing of energy usage data does not involve billing or energy supply to a particular household. A consumer could for instance provide information on thresholds of electricity usage per week without this being linked to a name, address or other identifier, nor to other behavioural data of the same household.

2.2.5 Metadata, semantic web and agreement technologies

Use of metadata to describe the data:[18] e.g. type of data; ground for processing; allowed purpose of processing per controller; consent for which purpose for which controller/processor; allowed recipients of the data; time stamps for release, processing operations, erasure; linkability; anonymisation etc. This is a rather elaborate way of implementing data minimisation.

Use of metadata to implement data protection policies: e.g. a prohibition to process data, unless certain conditions are met; an obligation to anonymise or erase after a specific time-slot or under specific conditions; permission to process data for specific parties etc. This may allow for a granulor type of control, especially if integrated with intelligent agents on the side of the user.

Making the concept of agreement operational for systems of computational agents, allowing artificial agents on the side of the consumer to communicate and interact on a machine-to-machine basis with agents on the side of suppliers, network operators, local suppliers (neighbours), ESCOs, acting on behalf of the consumer.[19] The goal would be to detect and address violations of data protection legislaton, and to implement a consumer's expressed or inferred privacy preferences.

If such systems work, they would enable much more than just data minimisation. This would enable consumers to become data prosumers in their own right, depending on the transparency of the back-end of the system.

2.2.6 Discrimination Aware Data Mining (DADM)

With regard to profiling and the implications of an outcome that induces prohibited (indirect) discrimination the techniques of discrimination aware data mining are important (DADM); these techniques provide transparency about bias within the data mining operations that fall within the scope of prohibited discrimination.[20]

DADM can provide a measure of back-end transparency on how people are being profiled.

2.2.7 User Centric Personal Data Ecosystem

Obviously all these solutions have drawbacks, often involving new data protection risks (both privacy, discrimination and security risks). It is clear that a more holistic approach is needed, especially with regard to profiling, enabling new business models that do no thrive on secrecy and manipulation. Actively engaging end-users by providing three types of transparency seems pertinent:

1. Back-end system transparency: who is processing what data where, how, when and sharing with whom; what knowledge is inferred how, shared with whom on what conditions; how could such knowledge impact a person. This is about auditability of automated processing and decision systems.
2. Front-end system transparency: how can a person interact with the back-end system without falling prey to unwarrented manipulation; how can a person figure out what

interactions can safely and securely be delegated to artificial agent technologies; how can a person ensure that potential risks of energy usage behaviours are correctly anticipated by client-side profiling technologies (inference machines) that e.g. integrate crowd sourcing.

3. Interface transparency: how can information overload be prevented; how can manipulation be prevented; how can visual analytics and the use of icons be employed to generate intuitive interfacing between front-end and back-end of the Smart Grid.

Such threefold transparency can help to empower final consumers to become partners in processes of data analytics, taking a more central role within the personal data ecosystem.[21]

2.3 GENERAL RECOMMENDATIONS

1. Think in terms of data flows instead of isolated discrete data; foresee whether de-anonymisation will reinstate identifiability and treat data streams that are susceptible to such de-anonymisation as falling within the scope of data protection legislation.
2. Make privacy and security an essential part of your business-model, do not treat them as costs but as a competitive advantage – especially in the long run.
3. Start from and reiterate Data Protection Impact Assessments.
4. Practice Data Protection by Design and by Default.
5. Develop software tools and hardware infrastructure that is innovative in terms of DPbDesign and by Default.
6. Develop business models based on DPbDesign and by Default.
7. Practice Security by Design, notably end-to-end encryption and secure authentication wherever possible.
8. Invest in recurrent software analyses.
9. Practice discrimination-aware data mining.
10. Base your trust management on trustworthiness.
11. Never underestimate the recurrent cost of safety and security.
12. Don't allow critical infrastructure to depend on volatile markets.
13. Create separate data streams for (1) critical infrastructure that protects the right to universal service, and (2) commercial value added services.
14. Design profile transparency in the back-end of the Smart Grid system.
15. Design intuitive interfaces that provide transparency about the potential consequences of sharing one's data (showing what profiles they match).
16. Design for profile transparency in the front-end of the Smart Grid system (allow consumers to play around with their data to figure out how they are matched).

3 EU LEGAL FRAMEWORK FOR THE ENERGY MARKET

This section aims to provide an overview of the current state of affairs from the legal perspective.[22] The focus will be on the implications of the profiling technologies that render the Grid a Smart Grid.

3.1 OBJECTIVES

3.1.1 Right of universal service

The EU legal framework for the generation, supply and distribution of energy is based on the concept of services of general economic interest (SGEI),[23] which obliges the Union and the Member States (MSs) to take care of 'a high level of quality, safety and affordability, equal treatment and the promotion of universal access and of user rights'.[24] This regards universal access to public services, even if they are provided by commercial enterprises. Sauter finds that 'the clearest functional definition of universal service is perhaps the following one:[25]

> It establishes the right of everyone to access certain services considered as essential and imposes obligations on service providers to offer defined services according to specified conditions including complete territorial coverage and at an affordable price.'

Directive 2009/72/EC for the electricity market (see 3.1.4) opens with a universal service provision in art. 3.3:

> Member States shall ensure that all household customers,and, where Member States deem it appropriate, small enterprises (namely enterprises with fewer than 50 occupied persons and anannual turnover or balance sheet not exceeding EUR 10 million), enjoy universal service, that is the right to be supplied with electricity of a specified quality within their territory at reasonable, easily and clearly comparable, transparent and non-discriminatory prices. To ensure the provision of universal service, Member States may appoint a supplier of last resort. MemberStates shall impose on distribution companies an obligation to connect customers to their network under terms, conditions andtariffs set in accordance with the procedure laid down in Article 37(6). Nothing in this Directive shall prevent MemberStates from strengthening the market position of the household, small and medium-sized consumers by promoting the possibilities of voluntary aggregation of representation for that class of consumers.

Directive 2009/73/EC for the gas market (see 3.1.4) has a similar obligation in 3.2. In both cases this is complemented with a special protection for vulnerable customers, including a prohibition of disconnection in critical times.

3.1.2 Energy end-use efficiency

Directive 2006/32/EC, on energy end-use efficiency and energy services, introduces the need for improved energy end-use efficiency, the management of energy demand, the promotion of the production of renewable energy, reduction of CO_2 and other greenhouse gas emissions, stronger incentives for demand side energy services. To achieve such goals the Directive will be 'providing indicative targets as well as mechanisms, incentives and institutional, financial

and legal frameworks to remove existing market barriers (…)' and 'creating the conditions for the development and promotion of a market for energy services and for the delivery of other energy efficiency improvement measures to final consumers' (art. 1). This directive imposed the obligation on MSs to provide smart meters, I will return to this point below (section 3.2).

On 25th October 2012 Directive 2012/27/EU has been enacted, which will replace (amongst others) the current Directive 2006/32/EC. MSs have until 5th June 2014 to implement this Directive into national law. This Directive sets as a target the saving of 20% of the Union's primary energy consumption by 2020 compared to projections (art.1). This is part of the Europe 2020 Strategy and the flagship resource-efficient Europe. This Directive repeats the obligation on MSs to provide smart meters, see below in section 3.2.

The 2012/27/EU Directive aims to strenghten and increase policies for energy efficiency, notably integrating cogeneration of heat and power, (repealing Directive 2004/8/EC that now addressed this issue),[26] reinforcing measures to empower of final customers by providing access to actual energy consumption (smart metering, art. 9; energy audits and energy management systems, art. 8, including transparency about high-efficiency cogeneration; a consumer information and empowering programme, art. 12), and stepping up measures to facilitate and promote demand response (for instance by means of flexible pricing or automation). It sets exemplary targets for public bodies' buildings and for purchasing by public bodies and requires MSs to develop energy efficiency obligation schemes (art. 7). Theses energy efficiency obligation schemes e.g. entail 'new savings each year from 1 January 2014 to 31 December 2020 of 1.5% of the annual energy sales to final customers of all energy distributors or all retail energy sales companies by volume, averaged over the most recent three-year periode prior to 1 January 2013' (art.7.1). The Directive devotes specific attention to energy services (art. 18) by requiring MSs to promote the energy services market that should contribute to energy savings (e.g. by means of financial instruments, incentives, grants and loans; quality labels; certifications; model contracts; qualitative review).

3.1.3 Use of energy from renewable sources

Directive 2009/28, on the use of energy from renewable resources,[27] aims to contribute to compliance with the Kyoto Protocol, reducing dependence on imported oil, as well as promoting security of energy supply, technological development and innovation. Special attention goes to the energy market for the transport sector. A 20% share of energy from renewable sources and a 10% share for transport are set to be achieved by a just distribution of mandatory national targets by 2020.[28] A guarantee of origin is stipulated and regulated to achieve transparency and accountability.[29] The Directive also lays down rules for access to the electricity grid for energy from renewable sources: art. 16 stipulates that 'MSs shall take the appropriate steps to develop transmission and distribution grid infrastructure, intelligent networks, storage facilities and the electricity system, in order to allow the secure operation of the electricity system as it accommodates the further development of electricity production from renewable energy sources, including interconnection between MSs and between MSs and third countries. MSs shall also take appropriate steps to accelerate authorisation procedures for grid infrastructure and to coordinate approval of grid infrastructure with administrative and planning procedures'. The Directive requires reliability and safety of the grid, 'based on transparent and non-discriminatory criteria defined by the competent national authorities' [art. 16(2)]. MSs must 'assess the necessity to build new infrastructure for district heating and cooling produced from renewable energy sources in order to achieve the 2020 national target (…). Subject to that assessment, MSs shall, where relevant, take steps with a

view to developing a district heating infrastructure to accommodate the development of heating and cooling production from large biomass, solar and geothermal facilities' [art. 16(11)].

Note that the Directive requires 'intelligent networks', but hardly refers to the input of consumer-generated renewable energy into the grid.

3.1.4 Reform and common rules for the internal energy market

Directive 2009/72/EC, and Directive 2009/73, concerning common rules for the internal market for electricity (2009/72) and natural gas (2009/73) introduce a novel framework for the internal market in electricity with the aim of creating new business opportunities, more cross-border trade, efficiency gains, competitive prices and higher standards of service, while contributing to security of supply and sustainability (recital 1 of both Directives). The idea has been to create a level playing field for all electricity undertakings in the EC. One of the instruments to achieve this is a fully effective separation of network activities from those of the supply and generation of energy, hoping to remove incentives for vertically integrated undertakings. Next to this the Directive states that MSs *may* impose public service obligations with regard to security of supply, quality, pricing and environmental protection, energy efficiency, energy from renewable sources and climate protection, in art. 3.2 (both Directives), and requires MSs to promote energy efficiency by means of e.g. the introduction of smart metering systems or smart grids.

In the Annex the Directives ***require*** MSs to introduce smart meters and, if – after conducting a cost benefit analysis - they are cost effective, to have a rollout by 2022 covering 80% of end-users.

3.1.5 Summary

Based on the EU legislative framework we can define the following objectives for the internal EU energy market:

- Universal access to affordable energy for end-users
- Reliability and availability of energy
- Improved energy end-use efficiency (energy savings)
- Demand-response, based on adequate pricing strategies
- Generation of renewable energy resources, with a targeted outcome in 2020
- Reduction of CO_2
- Removal of existing market barriers (unbundling)
- Flexible pricing strategies
- Correct information for end-users regarding their energy usage and pricing
- Transparency for end-users about the share of renewable energy in their energy consumption

3.2 SMART METER

The Measuring Instruments Directive 2004/22/EC observes in Recital 2 that:

> Correct and traceable measuring instruments can be used for a variety of measurement tasks. Those responding to reasons of public interest, public health, safety and order, protection of the environment and the consumer, of levying taxes and duties and of fair trading, which directly and indirectly affect the daily life of citizens in many ways, may require the use of legally controlled measuring instruments.

This implies that smart meters must be 'legally controlled', in the sense of meeting legal requirements in terms of durability, accuracy, suitablity etc. This may, for instance, have consequences for the mandatory data retention capacities of smart meters. In Annex MI-003 (active electricity meters) the Directive stipulates under 5.3 that:

> In the event of loss of electricity in the circuit, the amounts of electrical energy measured shall remain available for reading during a period of at least 4 months.

Art. 13.1 of Directive 2006/32/EC [and art. 9.1 of Directive 2012/27/EU] determines that:

> MSs shall ensure that, in so far as it is technically possible, financially reasonable and proportionate in relation to the potential energy savings, final customers for electricity, natural gas, district heating and/or cooling and domestic hot water are provided with competitively priced individual meters that accurately reflect the final customer's actual energy consumption and that provide information on actual time of use.

The idea is that whenever existing meters are replaced, smart meters will be provided (also in the case of new or renovated buildings).[30] MSs must ensure that these meters enable billing based on actual energy consumption, while the following information must be provided to final customers:

a. current actual prices, actual consumption,
b. comparisons of current consumption with that of one year ago,
c. comparisons with average normalised or benchmarked usage,
d. contact information for consumers' organisations and similar bodies that can provide information on energy efficiency improvement measures.

The Art. 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Art. 29 WP) has written an Opinion (12/2011, WP 183) on Smart Metering in 2011. They note that Data Protection Supervisors responding to a questionnaire observed that 'the level of security needs to be comparable with other vast operation such as Internet banking' (idem: 2). They also note that without sufficient data protection 'there is a risk not only that processing of personal data will be in breach of national laws which implement Directive 95/46EC but also that consumers will reject these programmes on the basis that the collection of personal data is unacceptable to them' (at 3). The Art. 29 WP emphasizes that smart meters are 'a pre-requisite for the smart grid' (at 6).

The European Commission (EC) has issued a Recommendation on the rollout of smart metering systems (2012/148/EU) on 9th March 2012,[31] to which the **European Data Protection Supervisor (EDPS)** has responded with an Opinion (EDPS/12/10) on 11th June 2012. The Commission states:

> Recital 10**:** Data protection and information security features should be built into smart metering systems before they are rolled out and used extensively. Such features can effectively improve consumers' control over the processing of personal data.

To achieve such **Data Protection by Design**:

> Recital 9: (…) data protection impact assessments should make it possible to identify from the start data protection risks in smart grid developments.
>
> Recital (14) A template developed at Union level for conducting data protection impact assessments will ensure that the provisions of this Recommendation are followed coherently across MSs

The EC defines the smart metering system (art. 3(b) of its Recommendation 2012/148/EU):

> Art. 3(b) 'smart metering system' means an electronic system that can measure energy consumption, adding more information than a conventional meter, and can transmit and receive data using a form of electronic communication'.

The EC details its recommendation with regard to the **Data Protection Impact Assessment**, advocating Data Protection by Design and by Default. The EDPS has commented extensively on the Commission Recommendation. This will be further discussed under the heading of the European legal framework (section 3a.10).

Most important for this study is to acknowledge that while the Smart Metering System is pre-conditional for the rollout of the Smart Grid, the Smart Grid entails a more comprehensive system of energy generation, transport and distribution, introducing demand-response, flexible pricing and enabling added value services. One can image the provision of smart meters without further developing a Smart Grid, in which case the meter might reduce administrative costs due to its ability for remote reading and automated billing.[32] In fact, the Dutch report on social cost-benefit analysis (SCBA) of smart grids takes as its baseline the introduction of smart meters, followed up with active grid management and simplified control strategies.[33] This baseline scenario does not fall within the scope of the Smart Grid, but is enabled by the smart meter. So we should acknowledge that the smart meter is pre-conditional for the Smart Grid, but does not automatically generate a Smart Grid and has cost and benefits independent from the actual implementation of the Smart Grid.

3.3 STANDARDISATION

Interoperability is a precondition for a unified internal energy market, requiring technical and organisational standardisation. The European Commission has therefor addressed

- Mandate M/441 on smart meters (March 2009) to the European Standardization Organisations (ESOs): CEN, CENELEC and ETSI. The idea is to develop standards for an open architecture for utility meters with communication protocols enabling interoperability.[34] The ESOs have established the Smart Metering Coordination Group (SM-CG), which functions as a joint advisory body that provides a focal point concerning M/441. In December 2011 they published a Technical Report.[35]

- Mandate M/490 on Smart Grid deployment to the ESOs (March 2011), whose Joint Working Group published a Final report on Standards for Smart Grids in May 2011.[36] Additional reporting has been done in 2012, providing first recommendations for the reference architecture, a first set of consistent standards, sustainable processes and investigate standards for information security and data privacy.[37]

3.4 COST BENEFIT ANALYSIS

The Smart Grid Task Force Expert Group 2 on Smart Grids writes at the end of 2011: 'The course of Smart Grid adoption in Europe is far from clear. The underlying technologies remain expensive; their business case relies on assumptions of significant changes in customer behaviour; and cost-effective integration of existing systems and emerging technologies is not yet proven. The business model in many cases is still emerging, especially for customer applications, as regulators, utilities and third-party service providers define their roles and set technology standards. Many core systems remain unproven and currently a limited number of Advanced Metering Infrastructure (AMI) systems have been deployed in Europe.'[38] This is a sobering introduction to a detailed recommendation with regard to Data Handling, Data Safety and Consumer Protection. It highlights that cost-benefit analyses contain many uncertainties and require perhaps a precautionary approach to achieve robust knowledge of risks and opportunities.

Directive 2009/72/EU encourages MSs to deploy smart metering system (art. 3 of the Directive) 'that shall assist the active participation of consumers in the electricity supply market' (art. 2 of the Annex). 'The implementation:

> May be subject to an economic assessment of all the long-term costs and benefits to the market and the individual consumer or which form of intelligent metering is economically reasonable and cost-effective and which timeframe is feasible for their distribution. (…) Such assessment shall take place by 3 September 2012' (art. 2 of the Annex).

If the assessment is positive, 'at least 80% of consumers shall be equipped with intelligent metering systems by 2020' (art. 2 of the Annex). The Joint Research Centre (JRC) of the European Commission has recently published Guidelines for Cost Benefit Analysis of Smart Metering Deployment,[39] advising on both quantitative and qualitative assessment and their combination. In the Netherlands three Cost Benefit Analysis have been prepared, starting with the KEMA report of 2005, followed by a revised financial analysis and policy advice by KEMA in 2010, complemented with the Social Cost Benefit Analysis of CE Delft and DNV KEMA in 2012.[40]

Interestingly, the JRC has also written Guidelines for conducting a cost-benefit analysis of Smart *Grid* projects. This is linked to the EC Recommendation on smart metering 2012/148/EU, which reads:

> Recital 16: (…) the Commission considers it important to lay down criteria, a template and more general guidelines that would improve the depth and comparability of analyses. As suggested by the Smart Grid Task Force, the criteria should use quantifiable indicators.

The Recommendation stipulates in art. 31 that the economic assessment should always include the following four steps: tailoring to local conditions, CBA, sensitivity analysis,

performance assessment, externalities and social impact. The Guidelines for the CBA on Smart Grids also elaborate the proposal for a Regulation on guidelines for trans-European energy infrastructures, which provides a framework that should 'overhaul the existing Trans-European Networks for Energy (TEN-E) policy and financing framework'.[41] This Regulation will set rules to identify projects of common interest (PCIs) within a set of 12 strategic trans-European energy infrastructure corridors and areas; the Regulation will also provide a methodology and a process for the elaboration of a harmonised energy system-wide cost-benefit analysis for PCIs in electricity and gas. The proposal explicitly refers to smart grids as one of the priority thematic areas: 'adoption of smart grid technologies across the Union to efficiently integrate the behaviour and actions of all users connected to the electricity network, in particular the generation of large amounts of electricity from renewable or distributed energy sources and demand response by consumers'.[42] In its Guidelines the JRC follows the CBA model of the Electrical Power Research Institute (EPRI), as used in a report commissioned by the US Department of Energy. In response to the EC Recommendation on smart metering the European Data Protection Supervisor (EDPS) points out that the Data Protection Impact Assessment (DPIA) recommended by the Commission should be a part of the CBA.[43]

In this study I will not assess, evaluate or even discuss the intricacies of the CBA. However, we must acknowledge three points in relation to a calculation of costs and benefits.

First, as Andy Stirling has demonstrated,[44] the factors used to calculate either costs or benefits generally entail four types of incertitude: risks, uncertainty, ambiguity, and ignorance. As Stirling has demonstrated, risk analysis only pertains when there is certain knowledge about the probabilities of a factor's occurence and about the types of effects of that factor. This certainty allows precise calculation of costs and benefits. However, usually the incertitude refers to what Stirling defines as uncertainty (the knowledge about probability is not certain even though knowledge about the type of effects is certain); ambiguity (knowledge about probability is certain but there is no agreement about the effects, for instance about whether they are positive or negative); or ignorance (both the knowledge about the probability and that about the types of effects are incertain). In these three cases no precise calculations can be made. The complexity of introducing and developing a Smart Grid generates all types of incertitude. This indicates that a cost benefit analysis will depend on interpretation of the relevant factors and eventually requires political decision making. We must acknowledge that the quantification of incertitudes that refer to uncertainty, ambiguity or ignorance is either impossible or makes no sense.[45] In fact modelling and quantification inevitably reduce complexities. By mistaking uncertainties, ambiguities and unknown unknowns to calculable risks one takes the risk that the related threats become invisible when seen from the perspective of the CBA.

Second, from the perspective of behavioural economics Smart Meters that include a remote off switch present a major security risk. In the words of Ross Anderson and Shailendra Fuloria 'Smart meters change the game. The combination of commands that will cause meters to interrupt the supply, of applets and software upgrades that run in the meters, and of cryptographic keys that are used to authenticate these commands and software changes, create a new strategic vulnerability, (…)'.[46]

Third, the incertitude regarding security risks is related to the simple fact that critical infrastructure that depends on a computational layer will always require continuous monitoring, subsequent and sometimes real-time updating and recurrent upgrading. The amount of data to be processed within the context of the Smart Grid, as foreseen by the European legal framework will most probably require massive storage and processing power, thereby adding to the cost side of the CBA. It seems likely that the kind of computing power needed for central storage and processing will only be available if cloud computing is

employed.[47] Considering the fact that ICT expertise is both scarce and expensive while cloud computing will increase the demand for such expertise, one can safely predict that the costs of making critical infrastructure dependent on a computational layer will definitely be very high.

One way of keeping the risks of hacking, data breaches, system breakdown, interruption of availability and safety hazards as low as possible is to minimize the dependence on computational systems. In another paper Anderson and Fuloria draw important conclusions from this fact, while developing a first attempt towards a security-economics analysis:[48]

> Smart meters should by default only send such information to the utility as is necessary for billing and for technical operations. Information sharing with other entities – including energy management companies and the government – should require the customer's consent, or be done in accordance with the law. Laws requiring information sharing must be sufficiently narrowly targeted for the consumer to foresee their effects, and they must be proportionate and necessary in a democratic society.

Taking serious this advice from Anderson and Fuloria, I conclude that an economic analysis of the security dimensions of the Smart Meter results in the requirement of a clear separation between information necessary for billing & technical operations and all other information, taking into account that both concern personal data but the grounds for processing differ. Especially trading with data derivatives has inherent risks that should not burden the critical infrastructure.

An important question is whether these risks can be mitigated by supply demand matching in local grids of neighbourhood households, entailing distributed instead of central data storage, and employment of smart algorithms at the local level, thus disabling aggregate profiling and targeting by ESCOs.[49] It is not clear as yet how this relates to separation of data streams, notably those of the DNO, individual households, suppliers and ESCOs, especially when taking into account that various parties may combine these roles.

3.5 MARGIN OF APPRECIATION; LATITUDE OF MSS

Within the framework of European law, both the European Court of Justice of the European Union in Luxemburg and the European Court of Human Rights of the Council of Europe in Strassbourg reserve 'a margin of appreciation' for the MSs when interpreting EU legislation or the European Convention of Human Rights. This provides a measure of latitude for the MSs. Regarding EU Directives we can distinguish between minimum or complete harmonization. The first means that MSs adopt the minimum requirements of the Directive, but can add more stringent requirements. The second means that MSs adopt the precise requirements of the Directive without adding more stringent requirements, since this would obstruct the level playing field of the internal market. Also, in many cases MSs are allowed to add requirements or even to skip requirements if this is desirable from the perspective of environmental concerns.

The EU framework on Smart Grids seems to leave some room for deviation based on the different traditions around Grids in the MSs. As we have seen above, CBAs are to be conducted by MSs and they can - in theory - lead to the conclusion that in that particular MS the introduction of smart metering systems is not beneficial. For example, In Flanders the role-out has been halted on the basis of a cost benefit analysis, though this will be repeated and presently a roll-out has been initated by Eandis and Infrax.[50]

Alternatively the conclusion can be that in that particular MS the introduction requires a specific type of rollout, with perhaps different requirements. For that reason the Netherlands was able to codify the right for individual end-users to refuse a smart meter, in which case a 'dumb' meter must be provided without the capacity for remote reading. As mentioned above, the end-user can also request that the network operator does not perform remote reading, even if a smart meter is installed.[51] Such consumer rights have not been stipulated in the Directives regarding smart metering.

This confirms latitude for MSs regarding the introduction of the Smart Grid (since there will be no Smart Grid without a smart metering system): (1) deviation from the roll-out as promoted by the EU is possible on the basis of the outcome of the CBA and (2) on the basis of anticipated human rights violations.

4 EU LEGAL FRAMEWORK ON FUNDAMENTAL RIGHTS RELEVANT FOR THE SMART GRID

This section aims to confront current and future 'settings' of the EU legal framework on privacy, data protection and other fundamental rights, notably non-discrimination and due process. The focus will be on the implications of the profiling technologies that render the Grid a Smart Grid. Design implications will be indicated. They – obviously – require further study between lawyers, engineers, designers and business leaders.

4.1 DATA PROTECTION DIRECTIVE 95/46/EC AND PROPOSED REGULATION

The EU Data Protection framework was built on the Fair Information Principles as outlined in the OECD Guidelines of 1980.[52] The main legal instrument is the Data Protection Directive (DPD) of 1995 that requires MSs to implement its content into national law. This means that each MS has its own national Data Protection Act. Under the proposed General Data Protection Regulation (GDPR) Member States (MSs) will no longer have any latitude,[53] because the Regulation will have direct effect in all the MSs. For this reason I will discuss the main structure of the Directive, which returns in the upcoming Regulation and add subsequent changes, clarifications and additional requirements in the proposed Regulation.[54]

The proposed GDPR, to which I will refer as 'the proposed Regulation' or as 'the proposed GDPR', has been presented by the European Commission on 25th January 2012, together with a proposed Directive for Data Protection in the realm of policing and criminal justice (see section 3c). At the moment of writing this study, the proposed Regulation is still under discussion with the European Parliament (EP) and with the MSs. It is expected that most of the stipulations of the proposed Regulation will be agreed upon in the course of 2013.[55] Obviously part of the industry is lobbying against some of the new stipulations, notably against law enforcement, privacy by default, the right to be forgotten, stricter requirements of consent and data breach notifications. A lobbying document obtained via a Freedom of Information suit by the 'Europe-v-Facebook' NGO, written by Facebook to the Irish Data Protection Supervisor states in its introduction:[56]

> The new legislative framework should focus on encouraging best practice by companies like Facebook rather than on setting out detailed technical rules that will not stand the test of time and may be frustrating and costly for both service providers and users.

At this moment it is not expected that a major overhaul of the Regulation will take place in the course of the deliberations by the European legislator. The Regulation will enter into force the twentieth day after its publication in the EU Official Journal and take effect two years after that date. This implies that from 2016 data processing within the context of the Smart Grid will most probably have to comply with the new Regulation. It is crucially important for all stakeholders to anticipate its content.

4.1.1 Objectives

The objective of the 1995 DPD is twofold:

a) The protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data
b) The free flow of personal data within the internal market of the EU

It is important to note that the free flow of personal data is an independent goal of the directive; the idea is that data protection regimes must be harmonised to create a level playing field within the internal market of the EU. The proposed Regulation confirms these objectives.

4.1.2 Scope of application

The DPD stipulates that it is applicable when 'processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State' and e.g. also if 'the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community'.[57] This already implies a broad scope of application.

Some find that 'in practice, the Directive has by now become the international data protection metric against which data protection adequacy is measured'.[58] This is similar to the so-called 'California effect' within the US jurisdiction: to the extent that environmental law or the regulation of cyberspace affects parties outside the territorial jurisdiction of California or the EU, they may decide to comply with the most stringent legislation to prevent the hassle of having to develop granular compliance, depending on the applicable law.[59] Though there are limits to this effect, the proposed Regulation dares to grasp extraterritorial jurisdiction by stipulating that, besides being applicable to data processing by a controller or processor in the Union (art. 3 proposed Regulation):

> This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
> 1. The offering of goods or services to such data subjects in the Union, or
> 2. The monitoring of their behaviour.

As Goldschmidt and Wu argue in their *Who controls the Internet*, the mere fact that foreign companies want to do business in Europe will allow Europe to regulate activities of such foreign enterprises to the extent that they indeed impact European citizens.[60]

Design implications:

1. The introduction of a General Data Protection Regulation with direct legal effect in all the Member States entails that for all companies operating in the EU it becomes profitable to develop standards that articulate default compliance with EU data protection rights and obligations, since the legal requirements will be uniform across the EU.

4.1.3 Personal data

The current DPD is built around the processing of **personal data**. The definition of processing is very broad, including collection and storage in a database (even if not by automatic means). The definition of personal data is:

> any information relating to *an identified or identifiable natural person* ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [art. 2(a)].

Whether a natural person is identifiable depends on 'all the means likely reasonably to be used either by the controller or by any other person to identify the said person' [recital 26].[61] This criterion is casuistic, meaning that much will depend on the circumstances and e.g. the economic feasibility of using a data to uniquely identify a person.[62] Such economics will of course depend on the state of the art in technologies of de-anonymisation (costs) and on the incentive structure behind de-anonymisation. We may expect the costs for de-anonymisation to decrease due to the increasing availability of relevant techniques, increasing access to linkable data and commercial gain or governmental need for personal data.[63] Profiling technologies allow to correlate different data points, further facilitating the re-identification of de-anonymized data. In practice, this implies that data such as IP addresses, location and mobility data, RFIDs, but also anonymized energy consumption data may at some point allow for identification, even if they are not initially linked to a unique person. For a company it does not make sense to assume that such data are not personal data, because the risk that they will at some point render a person identifiable increases steadily with their correlatability. The advent of Big Data analytics, value added services and governmental fraud detection profiling implies that even the aggregation of smart meter data will not rule out identification. Attempts to avoid applicability of the DPD by means of de-anonymisation face three challenges: (1) to provide personalized energy services data must be contextualized, networked and enriched, which rules out anonymisation, (2) at the level of computing systems anonymity is not a categorical but a granular conception, depending not only on unobservability but also on unlinkability, and (3) whatever data is unobserved or unlinkable today may be correlated with other data tomorrow or ten years from now.

In that sense *any* (anonymous) data can become personal data, depending on the circumstances, economic incentives and technical state of the art. This should be taken into account when designing the Smart Grid. For the same reason it is better to think in terms of data flows instead of considering separate data; precisely because individual data of specific data streams may be or may become personal data it makes sense to treat all data within such a stream as personal data.[64] On top of that we must note that profiling techniques can infer sophisticated profiles from anonymous data. Though these profiles, patterns, association rules, correlations or nearest neighbours are not personal data, they become personal data once applied to an identifiable person. This relates to the right not to be subject to measures based on profiling and to the right to be informed of the existence of profiling and to be informed of the envisaged consequences of the processing involved in profiling. This will be discussed separately below.

I therefore propose to understand anonymisation, aggregation and/or encryption as implementations of Data Protection by Default (data minimisation) instead of ways to avoid applicability of the DPD or the proposed GDPR.

While this report was being prepared the LIBE draft report was released, presenting amendments to the proposed GDPR to be voted in the European Parliament (EP). The LIBE

is the EP Committee on Civil Liberties, Justice and Home Affairs. Though I will not discuss all suggested amendments, because it is unclear to what extent they will make it into legislation,[65] I make an exception for a proposed amendment in the definition of data subject. The LIBE proposes to redefine the definition as follows:

> any information relating to *an identified or identifiable natural person* ('data subject'); an identifiable person is one who can be identified ***or singled out***, directly or indirectly, ***alone or in combination with associated data***, in particular by reference to ~~an identification number~~ a ***unique identifier***, location data, online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social ***or gender*** identity or ***sexual orientation*** of that person;[66]

This is interesting in relation to energy usage behaviours because it would enlarge the scope of personal data to data that allow to re-recognize a person, e.g. based on linkability between different sets of data.

Design implications:

1. In the context of the Smart Grid all data streams that contain energy consumption behaviours should best be treated as personal data, even if data aggregation or other techniques for anonymisation have been implemented.
2. This means that for all data streams a Data Protection Impact Assessment is needed (see below) and Data Protection by Design and by Default (see below) must be implemented.
3. Note that in this view aggregation or anonymisation techniques can be viable implementations of DPbDefault, but do not render Data Protection legislation inapplicable.

4.1.4 Grounds and data minimisation: the conditions for lawful processing

This concerns two types of conditions: grounds for legitimate processing and rules on fair and lawful processing.

4.1.4.1 Grounds for processing.

Personal data may only be processed on one of six grounds (conditions):[67]

1. unambiguous consent of the data subject;
2. necessity for the performance or conclusion of a contract;
3. necessity to comply with a legal obligation for the data controller;
4. necessity for the protection of vital interests of the data subject;
5. necessity for the performance of a task carried out in the public interest or the exercise of official authority;
6. necessity for the purposes of the legitimate interests pursued by the controller, unless such interests are overridden by the fundamental rights interests of the data subject.

Design implications:

1. In the context of the Smart Grid it would be advisable to separate data streams based on necessity (contract, legal obligation, vital interests of the user, public interest, legitimate interests of the controller) from those based on consent.
2. Since consent can be withdrawn (see below), this does not provide for a stable data stream and fluctuating trust levels around value added service should not endanger the reliability of the Smart Grid or the availability of energy.

4.1.4.2 Data minimisation

Next to being based on a legitimate ground, data must also be processed fairly and lawfully.[68] This entails four requirements:

1. purpose specification;
2. use limitation;
3. accuracy and completeness;
4. deletion or anonymisation as soon as the purpose is no longer relevant.

These requirements are often summed up as **data minimisation:** only those data may be processed that are necessary to achieve the purpose of processing, which must be specified; they may not be used for other purposes without specific consent; they may not be used longer than necessary to achieve the purpose for which they were processed. The data controller, i.e. whichever person or organisation determines the purposes and means of processing [art. 2(d)], is responsible and liable for complying with these requirements [art. 6(2) and art. 23]. Below I will discuss the roles of data controller and data processor, their liability, and the various obligations they must perform in the Smart Grid.

Design implications:

1. Note should be taken that data streams based on consent or contract or any other legitimate ground must still comply with the conditions of data minimisation (i.e. purpose specification and use limitation, accuracy and completeness, and deletion or anonymisation as soon as the purpose is no longer relevant).

Proposals for Data Protection by Design and by Default:

a. It may save trouble to provide metadata for each data with the ground on which its processing is based, code for the purpose of processing and for the type of recipient of the data. This could make it easier to comply with transparency and auditability obligations and could fit with software that allows end-users to access their data in a format that easily sorts different types of data in a handsome overview.
b. To the extent that such metadata function as sticky policies that determine how they can be shared and used, they could implement data minimisation and fulfil the requirements of data minimisation. They could thus enable what the proposed Regulation means with 'Data protection by default'.
c. Special care should be taken to prevent that metadata generate more or more serious data protection vulnerabilities than they aim to solve.
d. Another option would be to put data in a personal data closet with an intelligent agent that checks, records, remembers, calculates which data are with whom/what

on what grounds, for what purpose, and which types of third parties may assess them.

e. In the contexts of the Smart Grid DPbDefault entails very strict default settings for the data stream of the critical infrastructure itself, preferably hardwired into the architecture.
f. At the same time it should provide similar – softwired - technical protection for data streams that nourish the applications of ESCOs, requiring them to clarify on the basis of machine-to-machine communication what data they need for what purpose, providing transparency for any secondary use (such as selling the data or data derivatives).
g. This could be combined with a software tool that allows only credentials for value-added services, e.g. integrated with a personal data vault, and an intelligent agent.

4.1.5 Data protection by default (DPbDefault) = Data minimisation by default

The requirements for fair and lawful processing are often summarized as requiring data minimization. This should be the default setting of the Smart Grid infrastructure.

The proposed Regulation stipulates in art. 23(2):

> The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

The Regulation further states that the Commission will 'adopt delegated acts (…) for the purpose of specifying any further criteria and requirements (…)' and sets out that 'the Commission may lay down technical standards for the requirements laid down in paragraph (…) and 2' [art. 23 (3) and (4)].

As mentioned above this translates the data minimisation principle into technical requirements, requiring devices and infrastructure that feed on data to always restrict themselves to data that are necessary for the purpose that is specified. So, whoever buys alcohol need not identify herself, but should merely provide proof of the claim that her age is over 18.

The Recommendation by the European Commission on the rollout of smart metering, defines DPbDefault as requiring: 'to implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage' [art. 3(e)]. The Recommendation further advices that 'for the purposes of optimising transparency and the individual's trust, MSs should encourage use of appropriate privacy certification mechanisms and data protection seals and marks, provided by independent parties' [art. 15].

Design implications:

1. In the contexts of the Smart Grid DPbDefault entails very strict default settings for the data stream of the critical infrastructure itself, preferably hardwired into the architecture.
2. At the same time it should provide similar – softwired - technical protection for data streams that nourish the applications of ESCOs, requiring them to clarify on the basis of machine-to-machine communication what data they need for what purpose, providing transparency for any secondary use (such as selling the data or data derivatives).
3. This could be combined with a software tool that allows only attributes/credentials for value-added services, e.g. integrated with a personal data vault, in the intelligent agent.

Have our cakes and eat them too?

1. In an environment where unexpected patterns may incentivize new business models and create unforeseen added value, data minimisation could stifle innovation.[69]
2. One solution for this problem would be to engage users, allowing their participation – based on enhanced transparency, open source software and intuitive interfaces that show what is done with their data and how matching profiles might impact them.
3. This will turn energy prosumers into data and profile prosumers[70], taking serious their participation in the creation of added value.
4. Profile-transparency, the right to forget and data portability are preconditional for such participation.

4.1.6 Sensitive data and discrimination

Sensitive data require a special regime, because their processing could allow for forbidden **discrimination**. D 1995/46/EC prohibits 'the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life' [art.8(1)]. The proposed Regulation adds criminal convictions or related security measures and genetic data to the category of sensitive data. Exceptions are possible in case of e.g. explicit informed consent, the vital interests of the data subject or specific legal obligations, but in principle processing on the basis of forbidden grounds of discrimination is not allowed.

In the case of profiling this is a very important prohibition, because if one detects a trivial data or an inferred pattern that correlates with ethnic origin or religious affiliation, it may be possible to work around the prohibition. Energy consumption patterns may indicate prayer times or fasting periods, linking with e.g. an Islamic background. They could also correlate with sexual preferences or criminal detention, if linked with other data. This could result in violation of discrimination in the context of occupation or employment (Directive 2000/78/EC) or racial discrimination (Directive 2000/43/EC).[71]

However, profiling notably enables refined price-discrimination, which is not prohibited and need not be based on sensitive data at all. It may, nevertheless create non-obvious and invisible types of discrimination which are unfair or otherwise undesirable. They may infringe upon the autonomy and identity construction of end-users of the Smart Grid and will be discussed separately under the heading of the 'Rights against unwarranted profiling'.

Design implications:

1. Profiling enables 'masking' [prohibited discrimination on the basis of trivial – non-sensitive – data that correlate with sensitive data].
2. To protect against 'masking' discrimination-aware data mining can be integrated.

3. Alternatively, an intelligent agent may be developed that can inference such correlations, and check via feedback loops and P2P communications with other agents whether such discrimination is indeed at stake.[72]

4.1.7 Consent

The Directive defines consent as 'freely given specific and informed' [art. 2(h)]. When the processing of personal data is based on consent, it must be given 'unambiguously' [art. 7(a)], and if consent is used to legitimate the processing of sensitive data the data subject must give 'explicit consent' [art. 8(2)a].[73]

The proposed Regulation specifies four conditions under which consent must be given to have legal effect:[74]

a. the burden of proof that consent has been given is with the controller
b. if consent is given in the context of a written declaration which also concerns other matter, it must be presented in a way that clearly distinguishes it from the other matter
c. consent can be withdrawn at any time
d. consent shall not have legal effect in the case of a significant imbalance between the positions of controller and data subject.

In the ePrivacy Directive – that contains the so-called cookie legislation – consent is required to track user behaviour by means of e.g. cookies.[75] This requirement does not depend on whether or not it involves personal data. Prior and informed consent is always required for behavioural targeting. This will be further discussed below, under the heading of the ePrivacy Directive and the Data Retention Directive.

In the context of profiling consent should not be overestimated as a legitimation. First, profiling can be based on anonymized data and still have a major impact once profiles are applied. In fact, under the current Directive and the proposed Regulation the application of profiles requires consent; per default one has the right not to be subjected to measures based on profiling (see below under 'measures based on profiling'). If profiles are applied, consent does not imply that the rules and principles for fair and lawful processing are no longer relevant. So, consent for being subjected to a measure based on profiling does not necessarily imply consent to process behavioural responses to such profiling (purpose limitation could be violated).

Design implications:

1. All services for which consent is required should be switched off by default.
2. A person should only give consent for the application of profiles if she is provided with the required transparency.
3. The consent switch should be granular enough to invite deliberate decisions but not overestimate the attention span of individual users:
    a. the switch must be easy to use for withdrawal of consent;
    b. on the basis of metadata built-in alarm signals should notify users of data and policy breaches and easy to understand notifications of changes in relevant policies or protocols, allowing for smart usage of the switch;
    c. different switches could be designed for data used to *construct* profiles and those used to *match* a person with existing profiles.

4.1.8 Rights of the data subject

One could, of course, qualify the requirement of consent as a right to consent of the data subject. But this is not very helpful. Consent is a condition. Irrespective of whether consent or one of the other conditions for the legitimate processing of personal data is applicable, data subjects have a number of rights.

Under the current Directive, end-consumers have a right to obtain from the network operator, their supplier: access to their data, information about their origin, the categories of data processed, the logic involved in any automated processing. These are generally called **transparency rights**. They also have a right to rectify, erase or block data if unlawful and they can require notification to third parties that hold data they have rectified, erased or blocked. These rights are sometimes called **participation rights**. End-users also have the right 'not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc' [art. 15(1)]. Various exceptions apply, notably in the case of a contract or authorization by law; in both cases the exception is only valid if suitable measures have been taken to safeguard the legitimate interests of the end-users. One could call these rights **against unwarranted profiling**.

The proposed Regulation entails basically the same set of transparency and participation rights, plus those against unwarranted profiling. However, some new rights have been added and some have been rearticulated. A right to data portability has been added and the right to erasure of one's personal data has been reinforced as the right to be forgotten. Finally the rights in relation to measures based on profiling have been reinforced, including an important transparency right regarding the envisaged effects of profiling. These rights will be discussed separately below.

Design implications under the current Directive:

- **Transparency** tools must be developed to provide end-users with easy to access to:
  - their data
  - information about their origin (where the data provided or automatically recorded)
  - a simple overview of the categories of data processed
  - the logic involved in any automated processing.[76]
- These software tools should integrate **participation** functions that enable end-users to:
  - rectify
  - erase or
  - block data if unlawful and to
  - require notification to third parties that hold data they have rectified, erased or blocked.
- Tools must be developed and/or integrated that protect against **unwarranted profiling:**
  - tools to disable unlawful profile matching
  - tools to exercise privacy protection, non-discrimination and due process rights in the case of decisions based on lawful profiling

4.1.8.1 The right to be forgotten

The proposed Regulation stipulates that a data subject has the right to obtain the erasure of her personal data, from the data controller, who must also abstain from further dissemination of such data, especially regarding data from when she was a child. This 'right to be forgotten' applies on one of four grounds: if the data are no longer necessary based on the purposes for which they were collected, lawful withdrawal of consent (if no other ground applies), lawful objection to the processing of her personal data and if processing is not in compliance with the Regulation for other reasons.[77]

1. If the controller had made the relevant data public, it must take all reasonable steps, including technical measures, to inform third parties that are processing such data that the data subject has requested erasure of any links to, or copy or replication of the data. If the controller has authorised a third party publication of personal data, the controller is deemed responsible for the publication.
2. The controller shall carry out the erasure without delay, except in the case of five specified exceptions: freedom of expression; public interest in the area of public health; historical, statistical and scientific research; compliance with a legal obligation based on Union or MS laws; or in the cases that the controller must restrict the processing of personal data.
3. In four specified cases the controller must restrict instead of erase data: if the accuracy is contested; if the data are no longer needed for the original purpose but must be kept for the purpose of proof; if the processing is unlawful but the data subject requests for their use to be restricted instead of erased; if the data subject requests to transmit the data into another automated processing system (data portability). In these cases the Regulation specifies how the data may still be processed. If the controller lifts the restriction the data subject must be informed.
4. Time limits for erasure or review of the need to continue storage shall be implemented by means of relevant mechanisms, by the data controller.
5. In the case of erasure the data shall not be otherwise processed by the controller.

The idea of a 'right to be forgotten' presents a strong metaphor. It reinforces the current 'right to have one's personal data erased' whenever the conditions for lawful processing are exhausted. Books have been written on the virtues of forgetting in the virtual age.[78] We must highlight the fact that values such as individual liberty require that individuals are not forever matched with their past behaviours. Reducing people to inferences from historical data could stifle the creativity triggered by effective privacy rights that allow people to reinvent themselves. Also, secondary use of behavioural data easily endorses unwarranted function creep that can only be mitigated if less data is available and people regain a measure of control over who 'knows' what about them on the basis of what data derivatives.

The proposed Regulation uses the term erasure, which clarifies that data should not merely be archived. Questions, however, remain as to whether anonymisation, aggregation or hiding from search engines, qualify as erasure.[79]

Design implications:

1. The proposed Regulation requires mechanisms to have personal data deleted; this means that the architecture should entail DPbDefault: automated deletion as soon as data minimisation requires it.
2. The proposed Regulation requires mechanisms to facilitate easy access of data subjects to their data, and easy implementation of their right to have data deleted in case of withdrawal of consent or unlawful processing.

3. The proposed Regulation requires mechanisms to delete data after having provided them in function of data portability.
4. The term 'mechanism' is not defined in the Regulation but should be understood in a broad sense, it seems to refer to a mix of automated or semi-automated procedures, protocols, standards, certifications, software tools that generate a default setting for specific operations.
5. In the case of the right to be forgotten, mechanisms should enable sophisticated, flexible consent management, e.g. by means of visualisation techniques, or sticky policies (with time stamps) combined with theorem provers.[80]
6. The to-be-deleted data that reside with third parties must be targeted to make the right effective, implying the use of e.g. the Semantic Web to chase one's data across the web.

4.1.8.2 Data portability

The proposed Regulation stipulates that data subjects have the right to obtain from the controller a copy of personal data undergoing processing. This right depends on whether the data are processed by electronic means in a structured and commonly used format. The data should be provided in an electronic and structured format commonly used to allow further use by the data subject.

If the data has been provided by the data subject and processing is based on consent, the data subject has the right to transmit them to another automated processing system – without hindrance from the original controller from whom the data are withdrawn.

This right should make it easy for end-user to switch supplier or to switch from one ESCO to another, while bringing her historical data to the alternative provider of energy or energy services. The idea is that the end-user should not be held hostage by a particular supplier or ESCO. Data portability could e.g. facilitate automated switching from one provider to another, which could be an enabler for flexible pricing strategies. I assume that 'personal data provided by the data subject on the basis of consent or contract' would include energy usage data, and I assume that in connection with the right to be forgotten the energy supplier and/or the ESCO must delete the data it holds once the data have been made portable and transferred to the end-user. However, this will depend on whether other grounds for the processing of these data are available and valid (data may still be needed for billing, for instance). We must also realize that when switching supplier or ESCO, end-users may have no idea of how to handle portable data, meaning that data controllers will transfer the data directly from one supplier or ESCO to another. This may require extra security, to prevent one provider gaining access to the data of another provider. Alternatively

Design implications:

1. Data portability means that a data subject can obtain her energy usage data from the Distribution Network Operator (DNO) and/or supplier, or from the ESCO that was processing them.
2. The data must be provided in an electronic and structured format, e.g. via a secure online environment, or on a disc, or the data could be transferred straightaway to the new supplier or ESCO, or even deposited in a personal data vault.
3. Since the DNO is the party that transfers relevant data to the suppliers or to the ESCO, it is not clear what data portability could mean in relation to the DNO. Should we foresee a time when DNOs are in competition across MSs?

4. The system may be designed in a way that keeps the data in a personal data vault, giving the data subject control over who gets to access the data. In that case portability is not the issue, but the right to be forgotten by the previous supplier or ESCO remains pertinent.

4.1.8.3 Rights against unwarranted profiling

The Directive provides the right not to be subject to automated decisions that have a significant impact or legal effect (though exceptions apply). It also provides a transparency obligation for the data controller, formulated as the duty to provide the 'logic of processing' in case of – at least – such automated decisions.

The proposed Regulation pays even more stringent attention to what it now coins as 'measures based on profiling'. It states that natural persons have the right not to be subject to measures with legal effects concerning this natural person or measures that may significantly affect this natural person, when such measures are based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.[81]

The proposed Regulation formulates 3 exceptions: in the case of (1) contract (where a right to obtain human intervention may be required as an adequate safeguard), (2) Union law or MS law, or (3) in the case of consent (again only if the necessary safeguards are in place).

The proposed Regulation also stipulates that in the case of such exceptions an evaluation of a person may not be based solely on sensitive data. This relates to the right to non-discrimination as discussed above.

Finally, the proposed Regulation stipulates that in case automated decisions based on profiling are lawfully made, the controller must provide 'information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.' Paragraph 1 concerns measures with legal effects concerning a natural person with significant effect or meant to evaluate personal aspects or to analyse or predict health, work, etc.

The implications for the Smart Grid of this set of legal rights and obligations are:

1. Smart metering is based solely on automated processing. Within the context of the Smart Grid, smart metering will be used to analyse and predict a natural person's behaviour, economic situation, reliability, location, personal preferences (think of fraud detection, default on payment, energy consumption behaviour, energy consumption preferences, needed for load balancing, flexible pricing)
2. Smart metering will be based on a contract with the supplier, the first exception that allows for measures based on profiling:
    a. The request for the contract will be 'lodged by the data subject' and – to the extent that she is provided with energy – the contract will be satisfied.
    b. In relation to energy services based on a contractual relationship the same may be valid, depending on what it means to 'satisfy' the contract on the side of the energy service providers.

   c. It is unclear why only when there is no contract 'measures to safeguard the data subject's legitimate interests' must be implemented and it is unclear why only when there is no contract there is a 'right to obtain human intervention'.
3. Smart metering will be expressly authorized by a MS's law, the second exception that allows for measures based on profiling. This legal basis may define the relationship with the DNO. This law must stipulate suitable measures to safeguard the data subject's legitimate interests.
4. Smart metering may be based on consent if it concerns energy services outside a contract. Consent is the third exception that enables measures based on profiling. Relevant are
   a. the burden of proof
   b. the effective right to withdraw consent at any time [this may be an advantage compared to a contractual relationship]
   c. a potentially significant imbalance
   d. the provision of suitable safeguards [e.g. the right to human intervention as a due process right; prohibition of secondary use and the other requirements of lawful processing]
   e. the prohibition to process sensitive data, which requires extra safeguards if overruled by consent
5. In the case of a contract, a law or consent the following information obligations apply:
   a. Info on the type of processing on which the measure is based
   b. Which attributes, behaviours, variables have been used
   c. What aggregate and/or personalized profiles have been applied
   d. Info on the envisaged effects on the end-user
   e. How is the end-user categorized in terms of e.g. billing, payments, future pricing, credit rating, health-risks, political affiliation, earning capacity?

Design implications:

1. Profile transparency must be realised in the ***back-end system***, rendering the lawfullness of the data mining operations auditable – while taking into account trade secrets and intellectual property rights.
2. Profile transparency must be realised by means of attractive ***interfaces*** that allow users to access information about the way they are profiled and how this may impact them.
3. Profile transparency must be realised in the ***front-end of the system***, inviting users to interact with their profiles, understanding how their energy usage behaviour is interpreted by the profiling technologies.
4. Another possibility is to put data in a personal data closet with an intelligent agent (inference machine) that mines own data and those of peers and thus:
   a. inferences what profiles a user matches.
   b. e.g. advices to withdraw consent and/or to order erasure.

4.1.9 The roles of data controller and data processor

Under the Directive, data controllers determine the purpose of processing, whereas data processors merely implement whatever the data controller decides. This was a nice division of tasks 'in the old days', but seems to be quite out of tune with present day realities. As some authors suggest, 'rather than the 1970s perception of an identifiable and single-jurisdiction data controller, at best assisted by an equally identifiable data processor, nowadays the norm

is for multiple, multitasking, "cloud-residing" or "outsourced" processing actors, with complex task and liabilities partitioning among them'.[82]

The Regulation does not change the labeling of data controller and data processor, but takes into account that the same organisational entities may perform different functions with regard to the same data. This has consequences for the distribution of responsibility of joint controllers (to be arranged between them, art. 24) and for the responsibility of the processor (that will be considered as a controller whenever it oversteps its mandate, art. 26(4), turning it into a joint controller with the controller that mandated its original processing operations (art. 26(4) and 24).

Furthermore the Regulation enhances **auditing requirements** for the controller and processing, demanding extensive documentation of the data processing operations (art. 28), to be made available to the supervisory authority on request. This only goes for companies employing more than 250 persons. At the same time the current framework of notifications to the supervisory authority will be abandoned (art. 18-19 of D 1995/46/EC).

The current procedure of prior checking of 'processing operations likely to present specific risks' (art. 20 D 1995/46/EC) returns in art. 34 of the proposed Regulation, allowing a controller or processor to obtain prior authorisation, which should ensure compliance. In specific cases the supervisory authority must still be consulted (art. 34(2).

The Regulation also imposes the appointment of a data protection officer in the case of data processing by a public authority or an enterprise employing more than 250 persons, or in the case that the monitoring of data subjects is the core business of the controller or processor.

The European Task Force Expert Group 2 on smart grids distinguishes the following six actors: Transmission System Operators (TSOs), Distribution System Operators (DSOs), Energy Generators (e.g. micropower production, MPP), Energy Market Suppliers, Metering Operators, and Customers (industrial, building owners, residential customers). The art. 29 WP distinguishes 3 types of data controllers: Energy suppliers (market suppliers in terms of the Task Force), Network Operators (DSOs in terms of the Task Force) and Other parties (central transmission manager between meter and supplier; energy regulator that needs data for policy setting and research; third party service providers or ESCOs).

Depending on the role these entities fulfil within a particular MS, they will qualify as data controller of data processor. This depends on (1) whether they process personal data and (2) whether they determine the purpose of processing. It might be the case that TSOs may not process any personal data, whereas the question whether DSOs, Energy Generators or Metering Operators are data controllers will depend on the way things are organised. Energy suppliers will at some point process personal data for the purpose of billing, so it is clear that they are controllers. Whether Metering Operators are merely processors or joint controllers depends on their role within the Smart Grid.

Design implications:

These will be discussed under the heading of 'obligations' and 'liability' hereunder. It is important to note, at this point, that the question is *not* whether a company or a public body designates itself as either a controller or a processor. This will be established on the basis of *actual control and delegation*.

4.1.10 Obligations of the data controller and the data processor

Under the Directive, data controllers must inform data subjects of their identity, the purposes of processing, the recipients or categories of recipients of the data, the voluntary or obligatory nature of providing specific data, of their right to access, and of their right to rectify and to delete their data [art. 10 D 1995/46/EC]. Obviously, where the Directive stipulates rights of data subjects with regard to data controllers, these will involve obligations. The proposed GDPR stipulates those obligations directly under the heading of the rights of the data subject, opening this section with a general obligation, stating that [art. 11 proposed GDPR]:

1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subject's rights
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

This is an important reminder and in combination with the obligations of Data Protection by Design and Default these requirements should be met by inventing simple and easy to use software tools to concretize e.g. 'data access by design' or 'profile access by design'. The obligations will be discussed under the Data Protection Impact Assessment, Confidentiality & Security and Breach Notification, Data Protection by Design.

4.1.10.1 Data Protection Impact Assessment (DPIA)

The proposed Regulation stipulates a Data Protection Impact Assessment (DPIA), 'where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes (art. 33). This is a new requirement, compared to the Directive. Though this may involve bureaucracy, it should in fact allow for a serious investigation into potential infringements of fundamental rights and freedoms. This will provide incentives and opportunities to build protection into the design of the devices or infrastructure, thus lowering risks and costs at a later point in time.

A PDIA must be carried out whenever an application entails processing operations that

- perform systematic and extensive evaluations of personal aspects, analysing or predicting economic situation, location, health, personal preferences, reliability of behaviour, based on automated processing;
- regard sensitive data, epidemiological researches, surveys of mental or infectious diseases;
- monitoring of publicly accessible areas;
- personal data in large filing systems on children, genetic data or biometric data;
- operations for which the consultation of the supervisory authority is required.

The PDIA must contain at least a general description of the envisaged processing operations and an assessment of the risks to rights and freedoms, complemented with an assessment of the envisaged measures to address the risks. The controller shall seek the views of data subjects or their representatives.

As mentioned above, the European Commission has issued a Recommendation on preparations for the roll-out of smart metering systems.[83] This Recommendation clearly links the Digital Agenda with smart metering and the smart grid, recognizing the need for data protection, network and information security, and cyber security. It refers to the guidance provided by various Opinions of the Art. 29 WP 'for developing "best available techniques" to safeguard personal data and guarantee data security when data are processing in smart metering systems and smart grids' (Recital 8), urging MSs to stimulate and support 'security and data protection by design' in the early stages of development (Recital 11). Best available techniques are defined as referring 'to the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU data protection framework. They are designed to prevent or mitigate risks on privacy, personal data and security' [art. 3(f)].

The Recommendation announces a template for conducting a DPIA, that is defined as meaning 'a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes to be to carried by the controller or processor or the processor acting on the controller's behalf' [art. 3(c)]. The template will be developed by the Commission and submitted to the Art. 29 WP for its Opinion, within 12 months after publication of the Recommendation. This means we should expect the template by March 2013. MSs should ensure that the advice of the Art. 29 WP is taken into account and they should take care that entities processing personal data should consult the national data protection supervisor on the DPIA, finally they must ensure that the template is adopted by network operators and operators of smart meters.

As to the content of the DPIA the Commission recommends:

> 4. The data protection impact assessment should describe the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC, taking into account the rights and legitimate interests of data subjects and persons concerned.

In its Opinion,[84] the EDPS expresses doubts as to the soft law approach. Since the Recommendation does not have force of law it depends on voluntary application by the industry. The EDPS finds that various important data protection aspects are not fully addressed. Notably, it observes that:

> by analysing detailed electricity usage data it may be possible in the future to infer or predict – also on a basis of deductions about the way in which electronic tools work - when members of a household are away on holidays or at work, when they sleep and awake, whether they watch television or use certain tolls or devices, or entertain guests in their free-time, how often they do their laundry, if someone uses a specific medical device or a baby-monitor, whether a kidney problem has suddenly appeared or developed over time, if anyone suffers from insomnia, or indeed whether individuals sleep in the same room [point 19].

The EDPS reminds us that patterns can be used for energy conservation, but also for many other purposes and have a high commercial value, for instance enabling price discrimination. It is unclear whether the EDPS is only referring to individual profiles, constructed from the data of one particular household, or also takes into account profiles mined from anonymized

data. The EDPS applauds the recommendations of DPbDesign and DPbDefault but warns that the template for the DPIA should not be taken out of context and must always be interpreted with the relevant legal framework in mind. This is an important warning: I agree that law cannot be reduced to a template, even if a template can help to actualize its performance. Furthermore the EDPS calls on the Commission to assess whether legislative action is necessary to stipulate mandatory technological protection instead of merely recommending it. This seems pertinent, to create a level playing field for the industry. Finally, the EDPS finds that the DPIA should be part of the mandatory CBA, which reinforces the need to move the DPIA from soft law to real law.

Design implications:

1. Smart Grid initiators should not await the Commission's template but actively foresee the kind of impact the Grid may have on data protection rights and obligations.
2. They should envisage how alternative designs impact e.g.:
    a. data minimisation;
    b. meaningful consent;
    c. data portability;
    d. the right to forget;
    e. profile transparency.
3. Various types of user participation should be taken into consideration, and the ability of users to understand the implications of their choices as well as their monitored behaviour should be ensured.
4. Designs that allow for high frequency trading with energy consumption behaviours (and the inferred data derivatives) must be avoided or at least separated from the data streams of the critical infrastructure since they will not empower the end-user and may cause volatility and unpredictable disruption of energy supply.

4.1.10.2 Confidentiality & security by design and breach notification

Under the current Directive, those charged with processing the personal data within the Smart Grid may only do so 'on instructions from the controller, unless required to do so by law' [art. 16]. The controllers 'must implement appropriate technical and organizational measures to protect personal data (…)' [art. 17(1)]. In the case of security breaches that result in identity fraud, privacy infringements, individuals must be notified 'when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual', unless the provider demonstrates to the competent authority that is has taken appropriate technological protection measures. The telecom provider must always notify the competent authority of the breach. So far, the obligations relating to data breaches have been regulated in the ePrivacy Directive (art. 3), which only applies to providers of publicly available electronic communications services. Under the proposed Regulation, however, these obligations are extended to all data controllers (art. 31 of the proposed Regulation). The notification concerns breaches of personal data, 'when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject' (art. 32 of the proposed Regulation). Similar exceptions apply if the controller demonstrates appropriate technological protection measures.

In the case of the Smart Grid, based on remote readings, two-way communication and a massive amount of invisible machine-to-machine talk a high level of security and confidentiality is obviously required by the detailed information that is transported and inferred. In its Recommendation on the rollout of the smart meter, the European Commission

advices 'security by design', meaning that it should be built into the architecture, as part of Data Protection by Design:

> This should encompass measures to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination, access to or alteration of personal data [art. 24].

The Commission advices 'the use of encrypted channels as it is one of the most effective technical means against misuse' [art. 25]. It requires compliance with the 'security-relevant' standard developed by European standardisation organisations, referring to its mandate[85] M/490 and taking into account international security standards, notably the ISO/IEC 27000 series [art. 26].

Design implications:

1. End-to-end encryption seems indeed imperative. It is unclear to me why this is not mandatory law. Though it will not solve all problems, it will reduce a number of problems that will otherwise require extensive investment at a later stage.
2. Especially in the case of remote readings and wireless machine-to-machine communication between the Smart Grid and domotica, many security incidents can be prevented by imposing end-to-end encryption.
3. Security by Design seems to be a prerequisite for a resilient infrastructure, since the cost of security breaches and ensuing system breakdowns would be exponential.
4. As indicated above, while discussing the CBA, the economics of security warrant a separation of the data stream of the critical infrastructure from that of value added services.

4.1.11 Data Protection by Design (DPbDesign)

In the Recommendation of the European Commission for the rollout of the smart meter, the EC defines DPbDesign as requiring 'to implement, having regard to the state of the art and the cost of implementation, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of Directive 95/46/EC and ensure the protection of the rights of the data subject' [art. 3(d)].

The proposed Regulation stipulates a similar engagement with up-stream requirements engineering to ensure compliance with the rights and obligations of the Regulation. This will enforce business leaders to make data protection a part of their business plan.

It seems clear that DPbD will be a standard based on technical and economic feasibility, involving a measure of legal uncertainty and negotiation. Much will depend on the way the Commission will use its competence to negotiate and impose technical standards [art. 23.2 and 23.3 of the proposed Regulation].

Design implications are discussed at throughout the analysis of the Regulation.

4.1.12 Liability of the data controller and the processor for non-compliance

In the current EU legislation every person should be provided with a judicial remedy to complain about any breach of the rights guaranteed by the national law; the person should receive compensation from the controller for the damage suffered. Finally, MSs should adopt 'suitable measures to ensure the full implementation of the provisions of this Directive'. Many have concluded that the current legal framework 'has not been successful in ensuring that data protection requirements translate into effective mechanisms that deliver real protection'.[86] In its Opinion on the principle of accountability, the art. 29 WP has advocated a system whereby controllers must (1) take appropriate measures to comply with data protection legislation and (2) must be able to demonstrate that they have done so.[87] The emphasis in the proposed Regulation on documentation and auditing requirements, discussed above, seems to follow this lead. At the same time it should be clear that straightforward and substantial liability will be needed to level the playing field, allowing controllers to inscribe data protection in the core of their business models without suffering a competitive disadvantage. In its report on the uptake of Privacy Enhancing Technologies (PETs), London Economics founds that many businesses claimed that they could only afford to make serious investments in PETs if their competitors were forced to do the same thing.[88]

Under the proposed Regulation data subjects can lodge individual complaints about the processing of their personal data with the supervisory authority. If unsuccessful the data subject has the right to a judicial remedy; she can go to court to contest the decision of the supervisory authority. This is a matter of administrative law. Just like in the case of the Directive, a natural person also has a right to a judicial remedy against a controller or processor; she can sue for compensation of any damage suffered and hold the controller or processor liable under private law.

Next to this – under the Regulation - penalties and administrative sanctions can be imposed, which differ substantially from the vague and non-committal 'suitable measures' required by the Directive.

The administrative sanctions consist of :

1. fines of up to 25.000 EUR or 0,5% of the annual worldwide turnover for intentional or negligent non-compliance with the obligation to provide mechanism for requests by data subjects or for charging a fee for information where this is unlawful;
2. fines of up to 500.000 EUR or 1% of the annual worldwide turnover for intentional or negligent non-provision of transparent information, non-provision of access or rectification; non-compliance with the right to be forgotten; non-provision of a copy of personal data in electronic format or non-compliance with data portability; non-compliance with distribution of responsibility in the case of joint controllers; non-compliance with required documentation; non-compliance with the rules for freedom of information or the conditions for processing for historical, statistical and scientific research purposes
3. fines of up to 1.000.000 EUR or 2% of the annual worldwide turnover for intentional or negligent processing of personal data without a sufficient legal basis or in violation of the rules and principles of fair and lawful processing; a violation of the rules for processing sensitive data; non-compliance with an objection to measures based on profiling; non-adaption of internal policies to implement Data Protection by Design and by Default; not designating a representative within the EU; etc. etc.

The sanctions remind one of sanctions more usual in competition law. Basically the supervisory authority, which can impose these fines, becomes a very powerful player and

seems to be in a position to level the playing field by punishing those who try to game the system.

Design implications:

1. The liability of controllers and processors of personal data under the proposed Regulation will require the articulation of all mandatory rights and obligations of the data protection framework into the Smart Grid architecture.
2. Combined with
    a. the imposition of DPbDefault (data minimisation),
    b. DPbDesign (early uptake of all the relevant rules and principles in the architecture)
    c. the introduction of new rights such as data portability, and
    d. newly articulated rights such as the right to be forgotten and
    e. rights against unwarranted profiling

    the imposition of liability will force the industry to innovate on the basis of a level playing field.
3. Techniques, technologies, applications, hardware, code, software and protocols will be invented and/or reinvented to make data protection part and parcel of the business model of advanced smart environments.
4. The development of the Smart Grid will benefit from early investment into security and privacy by design, preventing rising costs of ICT maintenance and preventing dangerous fluctuations in consumer trust. Those who fail to comply will be out of business.

4.2 ePRIVACY DIRECTIVE 2002/58 AND THE DATA RETENTION DIRECTIVE 2006/24

The scope of the ePrivacy Directive is limited 'to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks' (art. 3).[89] This – in principle – excludes 'information society services', because the scope of the ePrivacy Directive is restricted to publicly available *transmissions* of communications. To complicate matters various parts of the ePrivacy Directive are deemed to address data processing outside publicly available electronic communications services in public networks, notably the prior informed consent required for cookies and unsolicited communications.[90]

The ePrivacy Directive contains a data breach notification that is now part of the proposed Regulation (see above), and it contains detailed opt-in requirements for the use of cookies for the purpose of marketing or targeted services. Notably, since 2009 the Directive requires prior informed consent for the use of cookies for value added services. This does not depend on whether the relevant data are personal data. Anonymisation therefore does not exempt from the obligation to inform and acquire consent, though it does exempt from the rules and principles on fair and lawful processing of personal data in the DPD. To the extent that added value is created by means of tracking mechanisms that resemble cookies the ePrivacy Directive is relevant for the Smart Grid. The art. 29 WP, for instance, explains that the term 'cookie' 'should not be regarded as excluding similar technologies', and goes on to analyse two exemptions from the requirement of informed consent, namely (A) when a cookie is used 'for the sole purpose of carrying out the transmission of a communication over an electronic communications network' or (B) when a cookie is 'strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'.[91] Since value added services on the Smart Grid fall within the scope of the cookie

legislation, any tracking mechanism used for such services that resembles cookie technologies will require prior and informed consent even if data are not considered personal data.[92]

At this moment it is not clear to me to what extent, in which cases and under what conditions smart grid data will be considered traffic data and/or location data in the sense of the ePrivacy Directive. This will depend on whether the transmission of data takes place via a public communications network and should be considered as publicly available communication services.[93] If Smart Grid data are communicated via publicly available communications services or transmitted via public communication networks, the Data Retention Directive will be also be applicable, requiring the retention of traffic data for a specified period of time (MSs have latitude between 6-24 months, the Netherlands has opted for 12 months). The goal of the Directive was to aid the investigation, detection and prosecution of serious crime. The art. 29 WP noted in its Opinion that 'Investigation, detection and prosecution of offences referred to in the Directive should not entail large-scale data-mining based on retained data, in respect of the travel and communication patterns of people unsuspected by law enforcement authorities'.[94] We should note that various Constitutional Courts have struck down either the Directive or its national implementation as a violation of their Constitution.[95] See also above (section 3a.8A) on the newly articulated 'right to be forgotten' in the proposed Regulation.

Design implications:

If energy usage behaviour data are transmitted by means of a publicly available communication service or network:

1. tracking mechanisms such as cookies require informed prior consent,
2. traffic data must be retained in accordance with the national law that implements the Data Retention Directive; such data must be accessible for law enforcement under strict conditions in specific cases.

4.3 Council Framework Decision 2008/977/JHA and the proposed Police and Criminal Justice Data Protection Directive

The recently adopted Council Framework Decision that regulates the Data Protection for police and criminal justice is only applicable to cross-border exchanges of personal data within the framework of police and judicial cooperation. It entails minimum harmonisation, meaning that MSs can provide a higher level of data protection than required by the Framework Decision. It is not valid for data processing in the national context of police and criminal investigation, which also does not fall within the scope of the general DPD. This evidently creates many gaps in protection and lack of legal certainty within the EU. The Framework Decision basically extends and restricts the framework of the DPD. Though both legal instruments focus on the processing of personal data, the role of consent of the data subject as well as various information obligations for those who process data are mitigated. This relates to the specific conditions under which data is exchanged and processed between police and justice authorities. Art. 3 highlights the principles of lawfulness, proportionality and purpose. It e.g. stipulates that 'personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes' and 'may be processed only for the same purpose for which data were collected' and 'shall be lawful and adequate, relevant and not excessive in relation to the purposes fro which they are collected'. As mentioned above, the art. 29 WP has warned, in its Opinion on data retention, that the usage of traffic data should not involve indiscriminate profiling, but always be specific and involve the necessary safeguards. The protection of personal data in the sphere of criminal justice is

weak, due to the exceptions that are made to enable criminal investigation and security measures.

Similar exceptions are made in the draft Directive on data protection in the sphere of criminal justice. The proposed Police and Criminal Justice Data Protection Directive will, however, be applicable to data processing within the MSs, thus closing some of the gaps in the present system. But the level of legal certainty will be lower than desirable since MSs will have to implement the Directive into national legislation, allowing for latitude between MSs. As to content the Framework Decision and the Directive do not differ much. The European Data Protection Supervisor has expressed his concern about the new proposal for a Directive, with regard to: the lack of legal certainty about the further use of personal data by law enforcement authorities; the lack of a general duty for law enforcement authorities to demonstrate compliance with data protection requirements; the weak conditions for transfers to third countries; the unduly limited powers of supervisory authorities.[96]

It is a fact that Smart Grid data will at some point be accessed by police and justice authorities to conduct criminal investigations, and/or to use such data to detect e.g. social security fraud or tax evasion. Like in the case of access to traffic data on telephone or Internet traffic, and the interception of telephone content and telecommunications content, the temptation for justice and police to eavesdrop on the behaviours of their citizens will be substantial. Putting in place the necessary safeguards, such as those mentioned above, complemented with transparency and due process rights, is not only a matter of legislation. By designing the Smart Grid in a way that per default does not invite easy access to individual data, or to detailed group profiles based on artificial intelligence, unwarranted monitoring may be discouraged. Public private partnership should, in this case, not focus on how data mining based on consent within the private sector can be transferred to the public sector. It should – on the contrary - focus on how to prevent privacy, data protection, non-discrimination and due process to become empty shells. Systemic monitoring by justice authorities violates democratic standards and defies the safeguards of the Rule of Law; they undermine trust and may endanger the resilience of the Smart Grid. They are, however, not science fiction, as the Judgment of the German Federal Constitutional Court indicates, whereby it created a new fundamental right to the integrity and confidentiality of Information Technology Systems in response to legislation allowing intelligence operations that search computing systems by using malware (e.g. a Trojan horse).[97] The point of the Court was not that computer systems may never be 'hacked' by police or justice authorities, but that this should be restricted to specific instances that are foreseeable and conditioned by the necessary safeguards.

Design implications:

1. Smart grid operators should foresee that, especially in the context of fraud detection or tax evasion, law enforcement may seek ways to access energy usage data. This may concern either the usage data of a specific person, who is already under suspicion or Big Data that allow to create data derivatives deemed to aid criminal intelligence.
2. To the extent possible the architecture should prevent and rule out easy access to large amounts of energy usage data as this would be contrary to the principle of purpose binding. In individual cases and under strict legal conditions access should be enabled and it would help if the architecture has a default setting against easy access.
3. This is especially urgent for either specific personal data or Big Data collected by third parties who may be tempted to provide such specific or aggregated, anonymised data on a voluntory basis. Though this would obviously violate the legal requirements of data minimisation (purpose limitation, prohibition of secondary use without

explicit consent), it may be difficult to audit such violations after the data have been anonymised.

4.4 CLOUD COMPUTING AND THE TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA) & US APPROACHES TO ENERGY USAGE DATA

4.4.1 Cloud computing and the transfer of personal data outside the EEA

The Art. 29 WP writes about cloud computing as 'a global technological paradigm'.[98] The issue in this report is not whether Smart Grid providers will derive benefits from cloud computing, but focuses on the risks in terms of data protection. The art. 29 WP highlights the risks of a increased lack of control and insufficient information regarding the processing operations themselves:[99]

a. Lack of availability 'due to lack of interoperability (vendor lock-in)'
b. Lack of integrity 'caused by sharing of resources' (e.g. in case of conflicting interests)
c. Lack of confidentiality (notably in case of 'law enforcement requests made directly to the cloud provider')
d. Lack of transparency due to the complexity and dynamics of the outsourcing chain
e. Lack of intervenability (for the client and/or for the data subject) 'due to the complexity and dynamics of the outsourcing chain'
f. Lack of isolation (which would endanger unlinkability of personal data processed for different clients and jeopardize purpose limitation)
g. Lack of portability ('standard data formats and service interfaces')
h. Lack of accountability ('ability to establish what an entity did at a certain point in time in the past and how')

The Art. 29 WP notes that cloud clients are obligated 'to choose cloud providers that implement adequate technical and organisational security measures to protect personal data and to be able to demonstrate accountability'.[100] It is not entirely clear whether the Art. 29 WP is referring to public or private clouds or to both. This is relevant since they seem to have entirely different privacy and data protection implications.[101]

Special attention should be devoted to the transfer of personal data to third countries or international organisations. This is relevant insofar as network operators, energy suppliers or ESCOs make use of cloud computing, whereby data are transferred to data servers outside the territory of the EEA, or transferred to data servers run by companies that fall under a jurisdiction that may e.g. require them to share personal data with justice authorities outside the EU without notification to the relevant data subject. Though nobody is entirely clear about the risks of US Justice authorities requesting personal data held by US companies in data servers on the territory of the EU, it seems clear that governments outside the EU could indeed request and beget access to personal data.[102] Network operators, energy suppliers or ESCOs qualify as data controllers, whereas cloud providers qualify as data processors. This means that the Smart Grid providers are responsible for compliance with data protection legislation. Transfer of data outside the EU and the European Economic Area (EEA) may only take place 'the third country in question ensures an adequate level of protection'.[103] In relation to the US – which has a different framework of data protection that does not always comply with that of the EU – the US Department of Commerce has develop a so-called 'safe harbor framework', together with the European Commission. It allows US companies to

certify compliance with the US-EU Safe Harbor Framework, entailing compliance with the Directive. The art. 29 WP, however, considers that 'companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification'.[104]

The proliferation of private public partnerships (PPP) may at some point lead to governments requesting the results of high level data mining activities, to aid in the struggle against international terrorism, money laundering, child pornography or any other transnational crime. Even if this would be in violation of art. 25 and 26 of the current Data Protection Directive or art. 40-45 of the proposed Regulation, we might not be aware of such transfers and the trouble around the agreement on the transfer of EU air passengers' personal data to the US Department of Homeland Security and the EU-US agreement on financial data transfers via the SWIFT network are a case in point that compliance is not obvious.[105] The Art. 29 WP in fact finds that 'it is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority'.[106]

As to profiling, the problem would also be that knowledge mined from aggregated, anonymized Smart Grid data could be used against EU citizens traveling into the US or any other country that manages to gain access to such aggregate knowledge. In fact, such inferences are not personal data and thus not protected by the DPD or the Regulation. The transparency rights of art. 12 of the DPD and art. 20 of the proposed Regulation may apply to the application of such profiles, but the chance that we can exercise these rights can be deemed null and void when invoke across the EU borders.

Design implications:

4. Smart Grid operations that concern critical infrastructure should not be managed in public clouds for reason of energy availability, grid resilience and other security, privacy and data protection concerns.
5. Smart Grid applications that concern added value services should not be run in public clouds because of increased data protection risks.
6. To the extent that private clouds could provide benefits in terms of security, privacy and data protection, decisions on their employment and the relevant conditions should be part of the DPIA.

4.4.2 US approaches to energy usage data

As an afterthought it is interesting to note that within the Utilities Commission of the State of California has proposed to fund an 'Energy Data Center'.[107] In its whitepaper it makes a difference between (1) customer-specific data that would reveal personally identifiable information, which can only be obtained with a Non-Disclosure Agreement (NDA), and (2) aggregated and anonymous data. The paper mainly addresses the need for aggregated and anonymous data. Basically the paper suggests that 'by eliminating the utility as the gate-keeper for obtaining aggregated and anonymized data, it may allow for a more open process for governmental organizations and other researchers to obtain this type of data'.[108] Three possible roles are distinguished:[109]

1. Aggregate and anonymize customer-specific data such that it protects customers' privacy and make it available to the public in a timely manner
2. Provide independent research and analysis of current state, Commission, and utility programs using customer-specific data but publishing results of that analysis in an aggregated and anonymised form that protects customers' privacy
3. Facilitate the transfer of customer-specific data to a governmental organization, provided that governmental organization has an NDA with the Commission

The paper notes that customer usage data are confidential and disclosure requires written consent, unless this concerns 'generic information regarding the usage, load shape, or other general characteristics of a gropu or rate classification, unless the release of that information would reveal customer specific information because of the size of the group, rate classification, or nature of the information'.[110] However 'nothing […] shall preclude an electrical corporation or gas corporation from disclosing a customer's electrical or gas consumption data to a third party for system, grid, or operational needs, or the implementation of demand response, energy management, or energy efficiency programs, provide that […] the utility has required by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure, and prohibits the use of data for a secondary commercial purpose not related to the primary purpose of the contract without the customer's consent'.[111] The Utilities Commission has invited comments and schedule workshops to determine whether funding an Energy Data Center is in the public interest. It may be obvious that such a central data base raises a number of privacy issues, notably with regard to profile transparency.

This report cannot provide anything like a comprehensive account of US privacy law with regard to the Smart Grid. It is important to note that the US jurisdiction has a very specific and complex division of tasks and competences between federal and state legislations; applicability of federal privacy law is not certain; and note should be taken that privacy law is far less general than the EU legal framework of data protection legislation. Much is regulated at the level of specific branches of the industry and much is left to state legislation.[112]

4.5 THE MARGIN OF APPRECIATION FOR MSS

Since the proposed Regulation will unify EU law regarding data protection, the legal framework for the Smart Grid will not longer allow a margin of appreciation concerning data protection.[113] This is in fact one of the main goals of the Regulation: creating a level playing field within the EU internal market for energy generation, distribution and transportation. The measure of legal certainty should increase once all MSs are bound by the same rules, to be interpreted in a more consistent manner.[114]

The ePrivacy Directive and the proposed Police and Criminal Justice Data Protection Directive (replacing the Council Framework Decision) will continue to provide latitude for diversity between EU MSs. The EDPS laments the lack of legal certainty that will continue in the domain of law enforcement.

4.6 ART. 6, 8 AND 14 OF THE EUROPEAN CONVENTION OF HUMAN RIGHTS (ECHR)

It cannot be assumed that compliance with the Data Protection Legislation will automatically ensure compliance with the fundamental rights of privacy, non-discrimination and due process in the ECHR. These rights concern the relationship between the government and citizens, and are especially relevant with regard to both specific or more general access to data or data derivatives by law enforcement authorities. There is much to discuss here, but within the scope of this study, written for the Smart Energy Collective and not addressing the government, the focus is the Data Protection framework that clearly addresses private actors.

The Convention has direct legal force: it has to be applied by the MSs whether or not they have implemented legislation, and art. 13 requires that a right to an effective remedy is provided. Merely enacting a law is not enough for compliance, the substance of the relevant right must be protected. A resident in Europe can file a complaint with the European Court of Justice if she has exhausted all national legal remedies. This means that it may take many years to achieve success, but it also means that any person within the jurisdiction of the Convention who finds her rights violated can turn to the court and file a complaint against the relevant Member State.

4.6.1 Privacy

Art. 8 protects privacy, private life, home and correspondance.[115] The scope of this right is determined by the reasonable expectation of privacy at home, work, concerning family life and the content of any type of communication. Violation is only justified in the case of the following triple test:

1. There is a legitimate aim that is well specified and falls within the scope of one of the following aims: national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others;
2. The infringement is based on a law that is foreseeable, accessible, effectively implemented and containing the necessary and specified safeguards;
3. The infringement is necessary in a democratic society and proportial in respect of the legitimate aim.

We can assume that access to energy usage data is an infringement of privacy. This implies that any access by law enforcement must meet the requirements of the triple test. The obligations to fulfill these requirements rest with the government, but it is important that grid operators are aware of the fact that the human right of privacy is at stake and police, justice authorities, or any other governmental agency has to comply with art. 8.

4.6.2 Due process, fair trial

Art. 6 of the ECHR provides a set of specific rights in the case of a criminal charge.[116] These requirements concern the to a fair trial: a public hearing, before an independent tribunal, contradictory proceedings, equality of arms during the trail and immediacy of the presentation

of evidence. The main thrust of these requirements are that it allows a defendant to contest the charge, the evidence, but also the lawfullness of various methods of investigation.

Data collection by law enforcement authorities in the Smart Grid or the construction of criminal profiles based on data derivatives taken from Big Data in the context of the Smart Grid, may violate privacy. If a violation is not justified on the basis of art. 8 ECHR this can have specific legal effects, such as inadmissability of the charge, acquittal, or diminishment of punishment. The problem is that this only goes when the defendant's privacy was violated unlawfully, not when that of others has been violated. The second problem is that as long as data collected is not used in the court case, the violation may never surface.

Access to data for preventive purposes without a specific relation to a particular criminal offense will in general not be justifiable, though anonymisation may be deemed an adequate safeguard.

4.6.3 Non-discrimination

Art. 14 of the Convention stipulates a prohibition to discriminate 'on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status', when taking measures that violate their human rights to e.g. privacy or a fair trial.[117] This is of particular interest when criminal profiling data mining technologies are run on energy usage data, since they may lead to discrimination in the exercise of the right to privacy, the presumption of innoncence or other rights in the context of the fair trial.

4.6.4 Horizontal effect

Human rights protection stems from the need to protect individual citizens against the powers of the state, which are used to achieve such protection [this is called the paradox of the Rule of Law]. The relationship between citiens and state is generally seen as vertical, because the state has unilateral competence to decide the legal relations between citizens and between citizens and the state. To the extent that states have a positive obligation to protect citizens against violation of their human rights by other private parties, lawyers speak of the horizontal effect.[118] Especially in the case of private parties that provide critical infrastructure the state may be held responsible for not preventing violations of human rights by those involved in distributing, supplying and supporting public goods that require universal service.

This report, however, addresses those involved in creating a Smart Grid. Therefore the focus is on the rights and obligations of the generators, suppliers, distributors and consumers of energy in the context of the Smart Grid. Within the EU these rights and obligations are codified in the legal framework of data protection.

5 CONCLUDING STATEMENTS

The analysis in chapter 3 and 4 prepared an answer to the questions articulated in the introduction. The answer consistes of a set of design implications derived from the legal framework. These design implications have been summarised in terms of legal requirements and proposed technical solutions in chapter 2. In this chapter the answers to the questions are briefly taken up as concluding statements.

The first question was:

> Which should be the requirements for the complex network of machine-to-machine interactions within the Smart Grid so as to prevent illegitimate and unlawful violations of privacy law and data protection legislation?

This question has mainly been answered by an analysis of the current and upcoming legal framework on privacy and data protection within the EU. The legal requirements can be summarised in terms of three sets of rights and obligations. First, the obligation for the data controllers to perform a data protection impact assessment whenever the implications of data processing constitute substantial risks for rights and freedoms of energy end-consumers. Second, to implement data minimisation at the level of the architecture; this has been coined as data protection by default. Third, data controllers must implement transparency and other obligations and ensure an effective right to be forgotten, an effective right to data portability and other relevant rights at the level of the architecture; this has been coined data protection by design. In chapter 2 the legal requirements and various potential technical solutions have been summarised in terms of these three sets of rights and obligations.

The first subquestion was:

> How is the right to profile-transparency articulated within the EU legal framework and how can this right be turned into an effective right without necessarily destroying business models based on value added services?

This question was answered in reference to the right for individuals not be subject to automated decisions, except on condition of a contract, a law or consent. Whenever such a condition is fulfilled, data controllers must provide transparency about (1) the existence of the automated decisions and (2) their envisaged effects for energy end-consumers. In chapter 2 this transparency has been discussed briefly in terms of back-end, front-end and interface.

This question was followed by a second subquestion:

> How can energy consumers be involved in such business-models as data prosumers, sharing the benefits of advanced data analytics?

Can we have our cakes and eat them too? In chapter 2 various architectural articulations have been proposed to enable energy consumers to become data and data derivative prosumers, under the heading of a user centric personal data ecosystem.

In section 2.3 a set of general recommendations is provided that advice how legal protection by design may be achieved in the Smart Grid:

1. Think in terms of data flows instead of isolated discrete data; foresee whether de-anonymisation will reinstate identifiability and treat data streams that are susceptible to such de-anonymisation as falling within the scope of data protection legislation.
2. Make privacy and security an essential part of your business-model, do not treat them as costs but as a competitive advantage – especially in the long run.
3. Start from and reiterate Data Protection Impact Assessments.
4. Practice Data Protection by Design and by Default.
5. Develop software tools and hardware infrastructure that is innovative in terms of DPbDesign and by Default.
6. Develop business models based on DPbDesign and by Default.
7. Practice Security by Design, notably end-to-end encryption and secure authentication wherever possible.
8. Invest in recurrent software analyses.
9. Practice discrimination-aware data mining.
10. Base your trust management on trustworthiness.
11. Never underestimate the recurrent cost of safety and security.
12. Don't allow critical infrastructure to depend on volatile markets.
13. Create separate data streams for (1) critical infrastructure that protects the right to universal service, and (2) commercial value added services.
14. Design profile transparency in the back-end of the Smart Grid system.
15. Design intuitive interfaces that provide transparency about the potential consequences of sharing one's data (showing what profiles they match).
16. Design for profile transparency in the front-end of the Smart Grid system (allow consumers to play around with their data to figure out how they are matched).

6 GLOSSARY

For reasons of precision the legal terminology is defined in accordance with the relevant legal text, when applicable.

Art. 29 Working Party

Art. 29 DPD: 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data. (…) It shall have advisory status and act independently. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission'.

Data controller

Art. 2.d DPD: 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.

Data Derivative

A data derivative is knowledge or information that is inferred or derived from a data set, based on patterns mined by means of computational techniques such as clustering, association rules, regression analyses, neural networks, reinforcement learning, unsupervised algorithms and the more. The data derivative is the result of what is usually termed artificial intelligence. It does not refer to the result of a query (retrieval of information first put into the database).

Data processing

Art. 2.b DPD: 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making

available, alignment or combination, blocking, erasure or destruction'.

Note that mere recording, collection but also anonymisation all fall within the scope of 'data processing'.

Data processor

Art. 2.e DPD: 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.

Data Protection by Default

Art. 23.2 proposed GDPR: 'The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals'.

Data Protection by Design

Art. 23.1 proposed GDPR: 'Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'.

Data Protection Impact Assessment

Art. 33 proposed GDPR: 'an assessment of the impact of the envisaged processing operations on the protection of personal data. (…) The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks,

safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned'.

Data subject:

Art. 2.a DPD: 'an identified or identifiable natural person'. Recital 26: 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'.

Due Process and fair trial

This right stems from the context of criminal procedure and refers to the right to contest a criminal charge. It includes: the right to an independent tribunal, to external and internal publicity, to contradictory proceedings, to the presumption of innocence, to equality of arms, and to immediacy during trial. In a broader sense due process refers to the right to contest the way one is treated whenever such treatment has a significant impact on one's life.

Non-discrimination

As a human right this refers to prohibited discrimination, i.e. discrimination on grounds such as race, ethnic origin, political opinion, religion or beliefs, trade-union membership, genetic profile, health, sex life, criminal conviction or other security measures. It is connected with the right to equal treatment and to the prohibition to process data revealing such characteristics (art. 8 of the DPD and art. 9 of the proposed GDPR).

Personal Data :

Art. 2.a DPD: '"personal data" shall mean any information relating to an identified or identifiable

natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

Privacy

The right to privacy is defined in a number of ways. Four dimensions impact the current understanding of privacy: (1) the right to be left alone, (2) control over the sharing or hiding of one's personal data, (3) freedom from unreasonable contraints on the construction of one's identity. Spatial, physical privacy is distinguished from informational privacy and decisional privacy. The right is closely linked to autonomy and identity and is mostly seen as an opacity right, because it shields citizens from transparency to governmental agencies, fellow citizens or corporations.

Profile transparency

Art. 20 proposed GDPR: 'a measure which produces legal effects concerning a natural person or significantly affects her, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular her performance at work, economic situation, location, health, personal preferences, realiability or behaviour', and which is justified by means of contract, law or consent, requires that the controller provides information 'as to the existence of processing for [such a measure] and the envisaged effects of such processing on the data subject'.

7 ABBREVIATIONS

AI	Artificial Intelligence
AIMA	Artificial Intelligence the Modern Approach
AMI	Advanced Metering Infrastructure
Art. 29 WP	Art. 29 Working Party
CBA	Cost Benefit Analysis
CEN	European Commettee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
DADM	Discrimination Aware Datamining
DNO	Distribution Network Operator
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
ECHR	European Convention of Human Rights
EDPS	European Data Protection Supervisor
EIA	US Energy Information Administration
EPRI	Electrical Power Research Institute
ESCO	Energy Service Company
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
FIP	Fair Information Principles
GOFAI	Good Old Fashioned AI
JRC	Joint Research Center
KDD	Knowledge Discovery in Databases
MSs	Member States (of the European Union)
NDA	Non-Disclosure Agreement (US)
DPbDesign	Data Protection by Design

DPbDefault	Data Protection by Default
GDPR	General Data Protection Regulation
OECD	Organisation for Economic Co-operation and Development
PPDM	Privacy Preserving Datamining
PDE	Personal Data Ecosystem
PPP	Private Public Partnership
SGEI	Services of General Economic Interest
SG-CG	Smart Grid Coordination Group (ESOs)
SM-CG	Smart Metering Coordination Group (ESOs)
TEN-E	Trans-European Network for Energy

8 ANNEX: EU LEGAL FRAMEWORK SOURCES

SMART GRID EU LEGAL FRAMEWORK

Portal European Commission with regard to Smart Grid: http://ec.europa.eu/energy/gas_electricity/smartgrids/smartgrids_en.htm

Portal European Commission with regard to the Agency for Cooperation of Energy Regulators (ACER): http://ec.europa.eu/energy/gas_electricity/acer/acer_en.htm

Right to universal service

Art. 14 and 106.2 Treaty on the Functioning of the European Union (TFEU) on services of general economic interest (SGEI) and on undertakings entrusted with SGEI, via: http://europa.eu/lisbon_treaty/full_text/index_en.htm

Art. 36 Charter of Fundamental Rights of the European Union (CFEU) on SGEI, via: http://www.europarl.europa.eu/charter/default_en.htm

Universal Service Directive 2002/22/EC that qualifies electronic communications networks as universal services and stipulates requirements for availability, rights of end-users and corresponding obligations for providers: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML

Energy efficiency

Portal European Commission on the Single market for gas & electricity: http://ec.europa.eu/energy/gas_electricity/internal_market_en.htm

Directive 2006/32/EC on energy end-use efficiency and energy services, via: http://europa.eu/legislation_summaries/energy/energy_efficiency/l27057_en.htm

Directive 2012/27/EU on energy efficiency, repealing Directives 2004/8/EC and 2006/32/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:315:0001:0056:EN:PDF

Renewable energy resources

Directive 2009/28/EC on the use of energy from renewable resources, via: http://europa.eu/legislation_summaries/energy/renewable_energy/en0009_en.htm

Reform and common rules for the internal energy market

Portal European Commission on Network Codes & Guidelines: http://ec.europa.eu/energy/gas_electricity/codes/codes_en.htm

Directive 2009/72/EC with common rules for the internal market for electricity: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0072:en:NOT

Directive 2009/73/EC with common rules for the internal market for natural gas: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0094:0136:fr:PDF

Standardization

Mandate M/441, Standardization Mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability: http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf

See also: http://www.cencenelec.eu/standards/HotTopics/SmartMeters/Pages/default.aspx

Mandate M/490, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment,
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

See also:
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf

Smart meter

Measuring Instruments Directive 2004/22/EC, via: http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21009b_en.htm

Art. 13.1 of Directive 2006/32/EC that conditionally obligates the roll-out of the Smart Meter, via: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0032:EN:HTML

Opinion 12/2011 on Smart Metering (WP 183) of the Art. 29 Working Party: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf

Smart Grids Task Force Expert Group 2 of the Directorate-General Energy, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection. Recommendation to the European Commission*, Brussels, 5 December 2011: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

Recommendation 2012/148/EC of the European Commisssion on the Rollout of Smart Metering Systems, containing in the Anness the Common minimum functional requirements for every smart metering system for electricity (see especially art. 42): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF

Opinion on the Commission Recommendation 2012/148/EC of the European Data Protection Supervisor EDPS/12/10, on 8 June 2012: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

Cost Benefit Analysis

Joint Research Centre of the European Commission (JRC) Guidelines for Cost Benefit Analysis of Smart Metering Deployment: http://ec.europa.eu/dgs/jrc/index.cfm?id=2820&dt_code=HLN&obj_id=734

JRC Guidelines for Cost Benefit Analysis of Smart Grid projects: http://ec.europa.eu/dgs/jrc/index.cfm?id=1410&obj_id=14810&dt_code=NWS&lang

Proposed Regulation on guidelines for trans-European energy infrastructure, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0658:FIN:EN:HTML

FUNDAMENTAL RIGHTS LEGAL FRAMEWORK

Charter Fundamental Rights of the European Union (CFEU)

CFEU: http://www.europarl.europa.eu/charter/default_en.htm

European Court of Justice: http://curia.europa.eu/jcms/jcms/j_6/

European Convention of Human Rights (ECHR)

European Court of Human Rights: http://www.echr.coe.int/echr/homepage_EN

Fact sheets on case law: http://www.echr.coe.int/echr/en/header/press/information+sheets/factsheets

Data Protection

Art. 8 CFEU on the Protection of personal data, via: http://www.europarl.europa.eu/charter/default_en.htm

General Data Protection Directive 95/46/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

ePrivacy Directive 2002/58/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

Council Framework Decision 2008/977/JHA for police and criminal justice, via: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0018_en.htm

Recommendation 2012/148/EC of the European Commisssion on the Rollout of Smart Metering Systems, containing Common minimum functional requirements for every smart metering system for electricity (advocating Data Protection Impact Assessment and Data Protection by Design: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF

Proposed General Data Protection Regulation of 25th January 2012: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Proposed Police and Criminal Justice Data Protection Directive of 25th January 2012: http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf

Opinion EDPS 7 March 2012 on the data protection reform package: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

Opinion EDPS 8 June 2012 on the Commission Recommendation 2012/148/EC: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

Opinion EDPS 16th November 2012 on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe': http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

Opinion 3/2006 (WP119)) of the Art. 29 WP on data retention: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_en.pdf

Opinion 2/2010 (WP171)) of the Art. 29 WP on behavioural advertising: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

Opinion 3/2010 (WP173)) of the Art. 29 WP on the principle of accountability: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Opinion 15/2011 (WP187)) of the Art. 29 WP on the definition of consent: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

Opinion 12/2011 (WP183) of the Art. 29 WP on smart metering: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf

Opinion /2012 (WP191) on the data protection reform proposals: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

Opinion 05/2012 (WP194) on the Cookie Consent Exemption: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

Opinion 05/2012 (WP196) of the Art. 29 WP on cloud computing: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Opinion 08/2012 (WP199) on further input : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp

Discrimination

Art. 13 CFEU on non-discrimination, via: http://www.europarl.europa.eu/charter/default_en.htm

Directive 2000/78/EC on discrimination in the context of occupation or employment: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0078:en:HTML

Directive 2000/43/EC on racial discrimination: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML

Art. 14 European Convention of Human Rights, via: http://www.hri.org/docs/ECHR50.html

Privacy

Art. 7 CFEU on respect for private and family life, via: http://www.europarl.europa.eu/charter/default_en.htm

Art. 8 European Convention of Human Rights, via: http://www.hri.org/docs/ECHR50.html and http://www.echr.coe.int/Library/DIGDOC/Roagna2012_EN.pdf

Factsheet Case Law European Court of Human Rights on data protection: http://www.echr.coe.int/NR/rdonlyres/4FCF8133-AD91-4F7B-86F0-A448429BC2CC/0/FICHES_Protection_des_données_EN.pdf

Factsheet Case Law European Court of Human Rights on anti-terrorism measures: http://www.echr.coe.int/NR/rdonlyres/13BF0C6A-F463-4CE9-B79F-9E9F3EF67B8F/0/FICHES_Terrorisme_EN.pdf

Fair Trial

Art. 47-50 CFEU on the rights to an effective remedy and to a fair trial, presumption of innocence and right of defence, principles of legality and proportionality of criminal offences and penalties, right not to be tried of punished twice in criminal proceedings for the same criminal offence, via: http://www.europarl.europa.eu/charter/default_en.htm

Art. 6 European Convention of Human Rights, via: http://www.hri.org/docs/ECHR50.html and http://www.echr.coe.int/Library/DIGDOC/Vitkauskas2012_EN.pdf

Notes

[1] Two earlier versions of this report were discussed in the Privacy & Security Working Group of the Smart Energy Collective in the course of 2012. I thank all participants for their stimulating, critical and open discussion of the contents. Interdisciplinary collaboration is not obvious but exceedingly necessary. I like to thank Marko van Eekelen and Erik Poll of the Institute of Computing and Information Sciences (iCIS), Radboud University, Frederik Zuiderveen-Borgesius of the Institute voor Informatie Recht (IViR), University of Amsterdam, Jennifer Urban of Berkeley Law, University of California for reading and commenting earlier versions of the report. Any remaining mistakes are my own.

[2] Though they will often be the same companies who also supply energy. This is a risk for data protection, since it will require deliberate design interventions to comply with purpose limitation. E.g. ENECO, http://thuis.eneco.nl/energie-besparen/toon-thermostaat/ and http://eneco.custhelp.com/app/answers/detail/a_id/6567. ENECO indicates that energy usage data are stored anonymously to better compare them, but also indicates that data are only stored locally and will not be available for ENECO. This is somewhat contradictory: I assume that energy usage data are aggregated and anonymised by ENECO to profile customers, do load balancing etc, whereas the same data are stored as personal data in the local device.

[3] Balancing refers to the image of the scale: freedom infringements should be balanced by effective safeguards such as judicial control, limitation in duration, scope and invasiveness, accountability, transparency and the infringement must always be proportional to legitimate aim that is pursued with the measures that cause the infringement. On the image of the scale as that of a trade-off see the scrutinous analysis by Jeremy Waldron, "Security and Liberty: The Image of Balance", *Journal of Political Philosophy* 11, nr. 2 (juni 1, 2003): 191–210, doi:10.1111/1467-9760.00174.

[4] In the Recommendation of the European Commission (EC) 2012/148/EU the Smart Grid is defined in art. 3(a).

[5] Thomas L. Friedman, "I Made the Robot Do It", *The New York Times*, augustus 25, 2012, sec. Opinion / Sunday Review, http://www.nytimes.com/2012/08/26/opinion/sunday/i-made-the-robot-do-it.html. The Economist, "Wireless health care. When your carpet calls your doctor", *The Economist* nr. Monday, April 12 (2010).

[6] Bill Vlasic, "A Test of Smart Cars Gets Under Way", *The New York Times*, augustus 21, 2012, sec. Business Day, http://www.nytimes.com/2012/08/22/business/a-test-of-smart-cars-gets-under-way.html."A Second Life for the Electric Car Battery", *Green Blog*, bezocht augustus 27, 2012, http://green.blogs.nytimes.com/2011/04/27/a-second-life-for-the-electric-car-battery/.

[7] See Opinion 12/2011 on smart metering (WP183) of the Art. 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Art. 29 WP) at p. 2.

[8] Louise Amoore, "Data Derivatives On the Emergence of a Security Risk Calculus for Our Times", *Theory, Culture & Society* 28, nr. 6 (november 1, 2011): 24–43, doi:10.1177/0263276411417430.

[9] Stuart Russell en Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3de ed. (Prentice Hall, 2009). Tom M. Mitchell, *The Discipline of Machine Learning* (Carnegie Mellon University, School of Computer Science, available at http://www-cgi.cs.cmu.edu/~tom/pubs/MachineLearningTR.pdf, 2006).

[10] Quentin Hardy, "Big Data in the (Heated or Cooled) Air Around You", *The New York Times*, september 4, 2012, sec. Technology, http://bits.blogs.nytimes.com/2012/09/04/big-data-in-the-heated-or-cooled-air-around-you/.

[11] This may be a regulatory problem, based on the Patriot Act's competence to seek access to relevant data. But it may also be part of hidden operations that – though perhaps illegal under EU legislation – nevertheless take place and will be exposed. See Nicole Perlroth, "Hackers Claim to Have 12 Million Apple Device Records", *The New York Times*, september 4, 2012, http://bits.blogs.nytimes.com/2012/09/04/hackers-claim-to-have-12-million-apple-device-records/.

[12] Mireille Hildebrandt, "Legal Protection by Design: Objections and Refutations", *Legisprudence* 5, nr. 2 (2011): 223–248, doi:10.5235/175214611797885693.

[13] See section 4.4 on potential risks and benefits of cloud computing.

[14] See for the use of a cryptographically secured vault in the context of demand response applications in the Smart Grid: S. Wicker en R. Thomas, "A Privacy-Aware Architecture for Demand Response Systems", in *2011 44th Hawaii International Conference on System Sciences (HICSS)*, 2011, 1 –9, doi:10.1109/HICSS.2011.24. A proposal for personal data vaults in general: Min Mun e.a., "Personal data vaults: a locus of control for personal data streams", in *Proceedings of the 6th International COnference*, Co-NEXT '10 (New York, NY, USA: ACM, 2010), 17:1–17:12, doi:10.1145/1921168.1921191. A proposal to use personal data vaults in the context of mobile phones: Katie Shilton, "Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection", *Commun. ACM* 52, nr. 11 (november 2009): 48–53, doi:10.1145/1592761.1592778. See on PCWorld: Personal Data Vaults Put You in Control of Your Data Online: http://www.pcworld.com/article/259187/personal_data_vaults_put_you_in_control_of_your_data_online.html. See a Dutch provider of a similar system: http://www.qiycorporate.nl/en/. See Chapter 4 Identity Vault Requirements of the Univeristy of Michigan Enterprise Directory and Identity Management System: http://www.itcs.umich.edu/mcommunity/requirements/4-IDVaultReqs.pdf.

[15] E.g. Liu Ying-hua e.a., "State-of-the-art in distributed privacy preserving data mining", in *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 2011, 545 –549, doi:10.1109/ICCSN.2011.6014329. Marina Blanton, "Achieving Full Security in Privacy-Preserving Data Mining", 2011, 925–934, http://dblp.uni-trier.de/rec/bibtex/conf/socialcom/Blanton11.

[16] Klaus Kursawe, George Danezis, en Markulf Kohlweiss, "Privacy-Friendly Aggregation for the Smart-Grid", in *Privacy Enhancing Technologies*, bewerkt door Simone Fischer-Hübner en Nicholas Hopper, Lecture Notes in Computer Science 6794 (Springer Berlin Heidelberg, 2011), 175–191, http://link.springer.com/chapter/10.1007/978-3-642-22263-4_10. , http://www.privacybydesign.ca/content/uploads/2012/04/pbd-smartmeters-europe.pdf. See a presentation by Cavoukian and Kursawe: http://www.ipc.on.ca/images/Resources/2012-08-29-IEEE.pdf.

[17] Jan Camenisch en Els Van Herreweghen, "Design and implementation of the *idemix* anonymous credential system", in *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02 (New York, NY, USA: ACM, 2002), 21–30, doi:10.1145/586110.586114. Patrick Morrison en Eduardo B. Fernandez, "The credentials pattern", in *Proceedings of the 2006 conference on Pattern languages of programs*, PLoP '06 (New York, NY, USA: ACM, 2006), 9:1–9:4, doi:10.1145/1415472.1415483. See e.g. Jacobs: http://www.ecp.nl/sites/default/files/bart_jacobs.pdf or Vullers: http://satoss.uni.lu/seminars/srm/pdfs/2012-Pim-Vullers.pdf.

[18] Using metadata to describe privacy policies, e.g. Marc Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments", in *UbiComp 2002: Ubiquitous Computing*, bewerkt door Gaetano Borriello en Lars Erik Holmquist, Lecture Notes in Computer Science 2498 (Springer Berlin Heidelberg, 2002), 237–245, http://link.springer.com/chapter/10.1007/3-540-45809-3_19. Using metadata to e.g. enforce privacy in online social networks, see S. Jahid e.a., "DECENT: A decentralized architecture for enforcing privacy in online social networks", in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2012, 326 –332, doi:10.1109/PerComW.2012.6197504. Examples of projects, research, papers: a Briefing paper Digital Preservation Europe: The Usage of Metadata in Public Administration, http://www.digitalpreservationeurope.eu/publications/briefs/uses_of_metadata_in_public_administration.pdf; on Search Security: Electronic health records privacy will require metadata scheme: http://searchsecurity.techtarget.com/Feds-Electronic-health-records-privacy-will-require-metadata-scheme.

[19] Sascha Ossowski, *Agreement Technologies*, vol. 8, Law, Governance and Technology Series (Springer 2013), , http://www.springer.com/computer/ai/book/978-94-007-5582-6. FP7 Project on Agreement technologies: http://www.agreement-technologies.org/project.

[20] Salvatore Ruggieri, Dino Pedreschi, en Franco Turini, "Integrating induction and deduction for finding evidence of discrimination", *Artificial Intelligence and Law* 18 (juni 5, 2010): 1–43, doi:10.1007/s10506-010-9089-5.

[21] "Personal Data: The Emergence of a New Asset Class", *Personal Data: The Emergence of a New Asset Class | World Economic Forum*, bezocht januari 6, 2013, http://www.weforum.org/reports/personal-data-emergence-new-

asset-class. “Rethinking Personal Data”, *Rethinking Personal Data | World Economic Forum*, bezocht januari 6, 2013, http://www.weforum.org/issues/rethinking-personal-data. See the paper by Ontario’s Privacy and Information Commissioner Ann Cavoukian on Privacy and the Personal Data Ecosystem: http://respectnetwork.com/2012/10/31/commissioner-ann-cavoukian-publishes-privacy-and-personal-data-paper/ and also the Personal Data Ecosystem Consortium (PDE), an industry driven consortium aiming for user-driven intelligence from personal data: http://pde.cc.

[22] See the site of the European Commission on the Single market for gas & electricity, containing information on the so-called Third package of legislation, Certification, Network Codes, Smart Grids, Traded energy markets etc.: http://ec.europa.eu/energy/gas_electricity/internal_market_en.htm.

[23] Art. 14 Treaty Functioning of the European Union (TFEU): Without prejudice to Article 4 of the Treaty on European Union or to Articles 93, 106 and 107 of this Treaty, and given the place occupied by services of general economic interest in the shared values of the Union as well as their role in promoting social and territorial cohesion, the Union and the MSs, each within their respective powers and within the scope of application of the Treaties, shall take care that such services operate on the basis of principles and conditions, particularly economic and financial conditions, which enable them to fulfil their missions.’ See also art. 106(2) of the TFEU: ‘Undertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in the Treaties, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned tot hem. The development of trade must not be affected to such an extent as would be contrary to the interests of the Union’, and art. 36 of the EU Charter on Fundamental Rights: ‘The Union recognises and respects access to services of general economic interest as provided for in national laws and practices, in accordance with the Treaties, in order to promote the social and territorial cohesion of the Union.’

[24] Protocol (no 26) On Services of General Interest art. 1 (interpretation of art. 14 of the TFEU). See also the Universal Service Directive 2002/22/EC that qualifies electronic communications networks and services as services that require availability throughout the Community, and stipulates rights of end-users and corresponding obligations of providers. This is of course highly relevant for the Smart Grid.

[25] Wolf Sauter, “Services of General Economic Interest and Universal Service in EU Law”, *SSRN eLibrary* (mei 1, 2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136105., quoting the White paper on services of general interest, COM(2004) 374 final, at 8.

[26] Art. 14 Directive 2012/27/EU. Art. 15.4(b) stipulates that MSs will require that under specified conditions transmission system operators and distribution system operators ‘provide priority or guaranteed access to the grid of electricity from high-efficiency cogeneration. Annex I develops general principles for the calculation of electricity from cogeneration, Annex II determines a methodology for determining the efficiency of the cogeneration process.

[27] Definition of energy form renewable sources: non-fossil sources, namely wind, solar, aerothermal, geothermal, hydrothermal and ocean energy, hydropower, biomass, landfill gas, sewage treatment plant gas and biogases [art. 2(2), Directive 2009/28/EC].

[28] Art. 3(1), 5-11 and the table in part A of Annex I provide the calculations for such distribution.

[29] Art. 15 Directive 2009/28/EC.

[30] ‘Provided’ does not imply that consumers can be forced to accept the meter, see C.M.K.C. Cuijpers en E.J. Koops, *Begluren en besturen door slimme energiemeters: een ongerechtvaardigde inbreuk op onze privacy*, Het wetsvoorstel “slimme meters”: een privacytoets op basis van art. 8 EVRM. Onderzoek in opdracht van de Consumentenbond (Tilburg: University of Tilburg, Oktober 2008). at 8.

[31] See the Annex for the ‘Common minimum functional requirements’ in art. 42 of the Recommendation.

[32] Cuijpers en Koops, *Begluren en besturen door slimme energiemeters: een ongerechtvaardigde inbreuk op onze privacy*., at 24-26. Cuijpers and Koops distinguish five objectives for the introduction of smart meters in the Netherlands: energy saving, energy availability, efficient administration, fraud detection and the ability to terminate the connection of end-user behind in payment. This correlates with five functions: measurement, switching, detection, communication and regulation.

[33] CE Delft en KEMA, *Maatschappelijke kosten en baten van Intelligente Netten* Rapport in opdracht van Ministerie van Economische Zaken, Landbouw en Innovatie (Delft, maart 30, 2012), http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/03/30/maatschappelijke-kosten-en-baten-van-intelligente-netten.html. Because Greenhouse horticulture and heavy industry are already fully equipped for Smart Grids, they are part of the baseline also.

[34] Cf. the website of CEN and CENELEC at http://www.cencenelec.eu/standards/HotTopics/SmartMeters/Pages/default.aspx. See also the OPENmeter project on Open Public Extended Network Metering Cooperation, with the objective: 'to specify a comprehensive set of open and public standards for AMI, supporting electricity, gas, water and heat metering, based on the agreement of all the relevant stakeholders in this area, and taking into account the real conditions of the utility networks so as to allow for full implementation', see at http://www.openmeter.com.

[35] Functional reference architecture for communications in smart metering systems (December 2011). Technical Report (CEN/CLC/ETSI/TR 50572:2011) approved by CEN and CENELEC, ftp://ftp.cen.eu/cen/Sectors/List/Measurement/Smartmeters/CENCLCETSI_TR50572.pdf.

[36] Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids, http://www.cen.eu/cen/Sectors/Sectors/UtilitiesAndEnergy/SmartGrids/Pages/default.aspx.

[37] See for ongoing work on standardisation for Smart Grids, by the CEN-CENELEC-ETSI Smart Grid Coordination Group, http://www.cencenelec.eu/standards/HotTopics/SmartGrids/Pages/default.aspx, and specifically on information security: CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security (2012), at ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf. The standards with regard to data privacy e.g. discriminate between sensistive personal information, personal information and no personal information; personal information is then categorized as de-personalized, pseufonymized or personal information. This allows for a granular treatment of energy usage data, depending on different levels of identifiability, pseudonymity and anonymity.

[38] Smart Grids Task Force Expert Group 2 of the Directorate-General Energy, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection. Recommendation to the European Commission*, Brussels, 5 December 2011, available at: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf.

[39] Vincenzo Giordano e.a., *Guidelines for Cost Benefit Analysis of Smart Metering Deployment* (JRC Institute for Energy and Transport, 2012), http://ses.jrc.ec.europa.eu/node/10.

[40] R.J.F. Van Gerwen, S.A. Jaarsma, en F.T.C. Koenis, *Domme meters worden slim? Kosten-baten analyse slimme meetinfrastructuur* KEMA Report (Arnhem: KEMA, augustus 2005). Rob Van Gerwen e.a., *Smart Meters in the Netherlands* Cost-Benefit Analysis requested by the Ministry of Economic Affairs, Agriculture and Innovation (Arnhem: KEMA, juli 13, 2010), http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/10/25/smart-meters-in-the-netherlands.html. CE Delft en KEMA, *Maatschappelijke kosten en baten van Intelligente Netten*.

[41] The Regulation is meant to replace Decision No 1364/2006/EC that lays down guidelines for trans-European energy networks. On 30th November the Council and the European Parliament reached informal agreement on the adoption of the regulation. It still needs formal approval in the Parliament (expected early 2013) and the Council (after the plenary vote in Parliament).

[42] Art. 123, ANNEX 1 of the proposed Regulation [/*COM/2011/0658 final - COM/2011/0300 (COD)*], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0658:FIN:EN:HTML.

[43] Opinion of the EDPS, 8 June 2012, on the Recommendation of the European Commission on smart metering.

[44] On the risk of risk-analysis: Claudio Ciborra, "Digital technologies and the duality of risk" (oktober 2004), http://www.lse.ac.uk/CARR.

[45] Andy Stirling, "Risk, uncertainty and precaution: some instrumental implications from the social sciences", in *Negotiating environmental change: new perspective from social science*, edited by Frans Berkhout, Melissa Leach,

en Ian Scoones (Cheltenham: Edward Elgar, 2003), 33–76. Stirling distinguishes 4 types of incertitudes: risks, uncertainties, ambiguities and ignorance (unknown unknowns). Only riks are fully quantifiable.

[46] R. Anderson en S. Fuloria, "Who Controls the off Switch?", in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, 96 –101, doi:10.1109/SMARTGRID.2010.5622026., at 96.

[47] On cloud computing see below, section 4.4.1.

[48] Ross Anderson en Shailendra Fuloria, "On the Security Economics of Electricity Metering", in *Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS)* (Cambridge, MA, USA, 2010), http://weis2010.econinfosec.org/papers/session5/weis2010_anderson_r.pdf. At 12/18. The quotation regards the first of five recommendations, the second stipulates open standards, the third stipulates that auditing energy usage that is billed to the energy supplier must be performed by the distributor, the fourth stipulates that demand management must be left to private contract between energy suppliers and their customers, the fifth requires an independent regulatory authority for smart grids that can and will stand up for the interests of energy users, ensuring both security of supply and market competition.

[49] E.g. G. K. H. Larsen, N. D. van Foreest, en J. M. A. Scherpen, "A price mechanism for supply demand matching in local grid of households with micro-CHP", *EPJ Web of Conferences* 33 (oktober 2, 2012): 01011, doi:10.1051/epjconf/20123301011.

[50] See M. Schrijner, W. Mulder and F. Koenis, *Financiële haalbaarheid slimme energiemeters in Vlaanderen. Een kosten-batenanalyse in maatschappelijk perspectief*, Arnhem 2012, Rapportnr.: 74100483-MOC/OPE 11-2641, available at www.vreg.be/sites/default/files/rapporten/kema.pdf. On the current roll-out, see the website of the Flemish Regulator of Electricity and Gas Markets: http://www.vreg.be/stand-van-zaken-slimme-meters#b (in Dutch). This roll-out is not obligatory, though this is not always made clear to consumers: Stefan Grommen, "Klant mag slimme meter weigeren" Knack.be, *Datanews.be*, oktober 2012, http://datanews.knack.be/ict/nieuws/klant-mag-slimme-meter-weigeren/article-4000186380716.htm.

[51] Art. 26ad, 26ac Electricity Act 1998, as amended March 2011.

[52] http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[53] In fact the European Court of Justice ruled on 24th November 2011 in cases C-468/10 and C-469/10 that art. 7f of the DPD does not allow MSs to impose either stricter nor less strict requirements.

[54] /* COM/2012/09 final */, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT.

[55] The Draft Report of the European Parliament, by Rapporteur Jan Philip Albrecht has been released, http://www.europarl.europa.eu/committees/en/libe/draft-reports.html?linkedDocument=true&ufolderComCode=LIBE&ufolderLegId=7&ufolderId=08739&urefProcYear=&urefProcNum=&urefProcCode=#menuzone. See e.g. earlier assessments by Fredirik Van Remoortel from law firm Crowell & Moring on the portal of Mondaq on 29 May 2012: http://www.mondaq.com/x/177058/Privacy/EU+Commission+proposes+new+Data+Protection+Regulation+including; and by W. Gregory Voss for the American Bar Association in *Business Law Today*, november 2012, available at http://apps.americanbar.org/buslaw/blt/content/2012/11/all.pdf.

[56] See http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

[57] See art. 4 Directive 95/46/EC for a precise articulation of the scope of the Directive.

[58] Paul De Hert en Vagelis Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review* 28, nr. 2 (april 2012): 130–142, doi:10.1016/j.clsr.2012.01.011.: 131.

[59] Vogel contrasts such an effect with the often assumed 'Delaware effect' that indicates a regulatory 'race to the bottom'. The Delaware effect, however, refers to a situation where states are 'legally required to recognize the legitimacy of one another's charters (an American version of mutual recognition)' which leads them 'to compete with one another by liberalizing their chartering requirements. The state which has been most successful in this competition has been Delaware'. Vogel, *Trading Up — David Vogel | Harvard University Press*, bezocht september 4, 2012, http://www.hup.harvard.edu/catalog.php?isbn=9780674900844., at 5-6. The California effect, however 'refers to the critical role of powerful and wealthy "green" political jurisdictions in promoting a regulatory 'race to the top' among their trading partners' (idem at 6).

[60] Jack Goldsmith en Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford University Press, USA, 2008).

[61] Referring to WP 183 on smart metering by the Art. 29 WP, the European Task Force Expert Group advices that most data from Smart Meters are to be considered personal data (Recommendation EG2.P.1). For extensive argumention concerning the types of data collected in the smart meter, see WP 183.

[62] In C-70/10 (SABAM v. Scarlet) of 24th November 2011 the EcJ seems to apply the theory that whether a type of data is personal data depends on whether the data controller has the ability to link the data with other data to which the controller has easy access. This entails a criterion of *relativity;* in the case of the Smart Grid it would probably mean that data controllers that can link energy usage data with identification must treat such data as personal data, whereas entities that cannot linke usage data with an identifiable person need not treat the data as personal data. As indicated in the main text, this is a risky approach that would require hardwired disconnection of both types of data, because once they are linkable de-anonymisation can easily become feasible.

[63] Paul Ohm, "Broken Promises of Privacy: Responding Tothe Surprising Failure of Anonymisation," *UCLA Law Review* 57 (2010): 1701–1777.

[64] This fits with Helen Nissenbaum's proposal to think in terms of contextual integrity instead of thinking in terms of isolated data. See Helen Nissenbaum, "Privacy as Contextual Integrity", *Washington Law Review* 79 (2004): 101–140.

[65] The LIBE draft report tends to extend the protection of personal data, whereas lobbying by the industry promotes self-regulation. It is expected that the proposed Regulation will be kept intact as much as possible to achieve a balanced outcome of the co-decision procedure of the EP and the Council of the European Union, see http://www.europarl.europa.eu/aboutparliament/en/0080a6d3d8/Ordinary-legislative-procedure.html and http://www.janalbrecht.eu/uploads/pics/data_protection_English.pdf.

[66] I thank Frederik Zuiderveen Borgesius for referring me to this specific proposal. See his speech in the EP, defending the amendment that extends 'identifiability' to being 'singled out', http://www.ivir.nl/publications/borgesius/Speech_EU_Parliament.pdf. See the Draft Report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) 2012/0011(COD), p. 63-64, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

[67] See art. 7 D 1995/46/EC for the precise articulation and conditions of the legitimate grounds.

[68] See art. 6 D 1995/46/EC for precise articulation.

[69] Betsy Massiello en Alma Whitten, "Engineering Privacy in a Age of Information Abundance", in *Intelligent Information Privacy Management* (AAAI, 2010), 119–124.

[70] See also Linda Steg, "Promoting household energy conservation", *Energy Policy* 36, nr. 12 (december 2008): 4449–4453, doi:10.1016/j.enpol.2008.09.027. on the types of incentives that do and do not generate user involvement or what she terms behavioural changes that achieve energy effeciency.

[71] Raphaël Gellert e.a., "A Comparative Analysis of Anti-Discrimination and Data Protection Legislations", in *Discrimination and Privacy in the Information Society*, bewerkt door Bart Custers e.a., vol. 3, Studies in Applied Philosophy, Epistemology and Rational Ethics (Springer Berlin Heidelberg, 2013), 61–89, http://www.springerlink.com/content/p91g6724n4v4w162/abstract/.

[72] For tentative examples see M Hildebrandt, *Behavioural Biometric Profiling and Transparency Tools* (Brussel: Future of Identity in Information Society, 2009), www.fidis.net.

[73] Unambiguous consent need not be explicit. This is obviously a matter of interprestation. If a website provides a banner stating that whoever accesses the site is deemed to agree to the use of tracking-cookies, a user who does access the site may be deemed to have provided unambiguous consent. However, this would not be explicit, which would require a deliberate intervention of the using to express consent. See also Art. 29 WP Opinion 15/2011 on the definition of consent (WP187), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[74] For precise articulation check art. 7 of the proposed Regulation.

[75] Directive 2002/58/EC, art. 5(3).

[76] However, this should not jeopardize trade secrets and/or intellectual property rights, though the protection of those rights should not render the substance of the transparency right entirely ineffective. See Recital 41: 'Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information'.

[77] This is a summary of art. 17(1) of the Regulation, sections 2-8 are summarized under the bullet points. For precision please check the full text version.

[78] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).

[79] Kieron O'Hara, "Can Semantic Web Technology Help Implement a Right to Be Forgotten?", *Computers and Law* (februari 2012), http://eprints.soton.ac.uk/273096/. , at 4.

[80] E.g. the VOME research project http://www.vome.org.uk/, or the ENCORE research projects: http://www.encore-project.info/.

[81] For the exact wording check art. 20 of the Regulation.

[82] De Hert en Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC". At 131.

[83] Recommendation 2012/148/EU.

[84] Opinion of the EDPS, 8 June 2012, on the Recommendation of the European Commission on smart metering.

[85] See Mandates M/441, http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf for smart meters and M/490 http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf for the Smart Grid.

[86] Art. 29 WP Opinion 3/2010 on the principle of accountability, WP 173, at 3.

[87] Idem, at 9.

[88] London Economics, *Study on the economic benefits of privacy-enhancing technologies (PETs) - Final Report to the European Commission DG Justice, Freedom and Security* (London: London Economics, 2010).

[89] The Art. 29 WP for this reason considers that geolocation tracking only falls under the scope of the ePrivacy Directive if the data is processed by telecom operators. Companies that provide apps using a combination of GOS,

WiFi and/or base station are qualified as 'information society service providers' and are thus excluded from the scope of Directive 2008/58/EC. Cf. Art. 29 WP 13/2011 on Geolocation service on smart mobile devices, WP 185.

[90] Cf. art. 29 WP Opinion 1/2008 on search engines WP148, section 4.13 and Opinion 2/2010 on behavioural advertising WP 171, section 3.2.1.

[91] Art. 29 WP Opinion 05/2012 on Cookie Consent Exemption, WP 194, referring to art. 5(3) of Directive 2002/58/EC.

[92] To check which data fall under the exemptions, smart grid operators can follow guideline 22 of the Recommendation of the European Commission on smart meters: 'Member States should perform an analysis prior to launching processing operations, in order to determine to which extent suppliers and network operators need to store personal data for the purposes of maintaining and operating the smart grid and for billing. This analysis should allow Member States to determine, inter alia, if the periods for the storage of personal data currently set in national law are no longer than necessary for the purposes of operating smart grids. This must include mechanisms to ensure that the time limits set for the erasure of personal data and for a periodic review of the need to store personal data are observed.'

[93] On the complexities of the applicable law for traffic and location data, see Colette Cuijpers en Bert-Jaap Koops, "How fragmentation in European law undermines consumer protection: the case of location-based services", *European Law Review* 33 (2008): 880–897.

[94] For a succinct overview of the safeguards that should be taken into account in case of data retention for purposes of criminal investigation, see art. 29 WP Opinion on data retention 3/2006, WP 119.

[95] Katja De Vries e.a., "The German Constitutional Court Judgement on data retention: proportionalisty overrides unlimited surveillance (doesn't it?)", in *Privacy and data protection: an element of choice*, bewerkt door S Gutwirth e.a. (Dordrecht: Springer, 2011). The legal ground and the applicable conditions for Justice Authorities to obtain access to traffic data are codified in art. 126n/126u and 126ng/126ug Dutch Code of Criminal Procedure.

[96] EDPS/12/7 of 7th March 2012, available at http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/12/7&format=HTML&aged=0&language=EN&guiLanguage=fr.

[97] German Federal Constitutional Court of 27th February 2008, BVerfG, NJW 2008, 822. See Wiebke Abel en Burkhard Shafter, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems - a case report on BVerfG, NJW 2008, 822", *SCRIPT-ed* 6, nr. 1 (2009): 106–123.The judgment did not stop the German police from engaging in similar unlawful operations, see e.g. Monika Ermert, German Police Used Trojan Horses in Investigations: http://www.ip-watch.org/2011/10/10/german-police-used-trojan-horses-in-investigations/.

[98] Art. 29 WP Opinion 05/2012 on Cloud Computing (WP 196), at 2. Cloud computing is defined (at 3) as consisting of 'a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Next to economic benefits, cloud computing may also bring security benefits; enterprises, especially small-to-medium sized ones, may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range.'

[99] Ibid 5-6 and 14-16.

[100] Ibid 14.

[101] On private clouds see http://www.vmware.com/nl/solutions/company-size/smb/server-consolidation.html, which provides a link to a video on virtualization of smart grid applications by Green Mountain Power in the US. The essence of cloud computing is virtualization, see http://www.vmware.com/nl/virtualization/virtualization-basics/what-is-virtualization.html. Also Ling Zheng, Yanxiang Hu, en Chaoran Yang, "Design and Research on Private Cloud Computing Architecture to Support Smart Grid", in *2011 International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, vol. 2, 2011, 159 –161, doi:10.1109/IHMSC.2011.109.

[102] W. Kuan Hon en Christopher Millard, "Data Export in Cloud Computing - How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Part 4", *ScirptEd* 9, nr. 1 (2012): 25–63.

[103] Art. 25.1 of Directive 95/46/EC.

[104] Ibid 18. See also on the possibility to include 'standard contractual clauses' as adopted by the EU Commission to frame international data transfers on a bilateral basis; as well as the possibility to adhere to the Binding Corporate Rules that constitute a code of conduct for companies that transfer data within their group (Ibid 18-19).

[105] For an overview: Christian Kaunert, Sarah Léonard, en Alex MacKenzie, "The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT", *European Security* 0, nr. 0 (0): 1–23, doi:10.1080/09662839.2012.688812.

[106] Art. 29 WP Opinion 05/2012 on Cloud Computing (WP 196), at 23.

[107] Thanks to Jennifer Urban for directing my attention to this. Audrey Lee, Marzia Zafar, for the California Public Utilities Commission, *Energy Data Center. Briefing Paper*, September 2012, see http://www.cpuc.ca.gov/NR/rdonlyres/8B005D2C-9698-4F16-BB2B-D07E707DA676/0/EnergyDataCenterFinal.pdf

[108] Ibid, 2.

[109] Ibid, 2-3.

[110] Ibid, 5.

[111] Ibid, 5-6.

[112] See e.g. http://www.smartgrid.gov/federal_initiatives/legislation. Basically States have competence to enact laws and regulations to cope with issues of privacy and data protection regarding customer energy usage data. According to US Energy Information Administration (EIA) in its report of December 2011 'Smart Grid Legislative and Regulatory Policies and Case Studies': 'three states (California, Colorado, and Oklahoma) have made significant progress in forming laws and regulations regarding smart meter data privacy'. See http://www.eia.gov/analysis/studies/electricity/pdf/smartggrid.pdf.

[113] See note 37 above, it seems that the European Court of Justice assumes that the DPD is meant to achieve complete harmonisation. Nevertheless, one Regulation with one text with direct effect in all the MSs will generate more legal certainty than the variety of national implementations so far.

[114] This refers to the so-called consistency mechanism prescribed in Chapter VI (Independent Supervisory Authorities) Section 2 (Consistency) of the Regulation (art. 57-63). Cp. the confusing situation under the current Directive, Art. 29 WP Opinion 8/2010 on applicable law, WP 179.

[115] See Ivana Roagna, *Protecting the right to respect for private and family life under the European Convention on Human Rights*, (Council of Europe human rights handbooks) (Strasbourg: Council of Europe, 2012).

[116] Dovydas Vitkauskas, *Protecting the right to a fair trial under the European Convention on Human Rights*, (Council of Europe human rights handbooks) (Strasbourg: Council of Europe, 2012).

[117] Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights: a guide to the implementation of the European Convention on Human Rights*, (Human rights handbooks ; no. 7) (Strasbourg: Council of Europe, 2007). at 58-59.

[118] Ibid 14-16.