



**00671/11/EN**

**WP 183**

**Opinion 12/2011 on smart metering**

**Adopted on 4 April 2011**

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 06/036.

Website: [http://ec.europa.eu/justice/policies/privacy/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/index_en.htm)

## **THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA**

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

**HAS ADOPTED THE PRESENT DOCUMENT:**

### **Introduction and Scope**

The objective of the Article 29 Working Party in this opinion is to clarify the legal framework applicable to the operation of smart metering technology within the energy sector. It is not the intention of this opinion to present a comprehensive view on all specific aspects of smart metering programmes across member states as the disparity of the current position does not allow us to do so. Smart meters offer new functionalities such as providing detailed information about energy consumption, the ability to remotely read the meter, the development of new tariffs and services based on energy profiles and the ability to remotely deactivate supply.

Smart grids offer even more scope for development and for the processing of more personal data. At this stage the Working Party does not intend to include smart grid functionality in the scope of this opinion. However, we would not rule out the further analysis of the smart grid when the picture is more developed.

The EC Directive on Energy End-Use Efficiency and Energy Services (2006/32/EC) sets energy saving targets to be adopted by each Member State. In order to achieve these targets and, subject to limited exceptions, article 13 of the Directive obliges Member States to provide consumers with meters that accurately reflect their energy consumption and provide information on actual time of use. These smart meters are

part of the attempt to meet the objectives of the European Union related to achieving sustainable energy supply by 2020.

Directorate-General Energy has set up a Task Force on smart grids. Expert Group 2, who form part of this Task Force, requested the assistance of the Article 29 Working Party to obtain a wider analysis of measures being implemented at a national level. To this end, in 2010, a questionnaire was circulated to data protection supervisory authorities. Six questions asked for views on smart grid developments (many of which are also addressed in this opinion). A further set of twelve questions requested information about the current state of smart metering implementation in member states. Those member states who responded to the six questions included observations that the level of security needs to be comparable with other vast operations such as internet banking. Answers to the set of twelve questions demonstrated that the implementation of programmes to roll out smart metering among domestic consumers of energy are relevant and urgent topics in many of the EU Member States. Smart metering is of particular significance in that it has the potential to affect the lives of almost all citizens as they all expect to receive a supply of electricity and gas. Its reach is extremely wide and is not restricted to those who have made a decision to engage with technological developments. The target is that coverage will be 80% of customers by 2020<sup>1</sup>.

Smart meters allow for the generation, transmission and analysis of data relating to consumers, much more than is possible with a 'traditional' or 'dumb' meter. Consequently, they also allow the network operator (also known as Distribution Service Operator or DSO), energy suppliers and other parties to compile detailed information about energy consumption and patterns of use as well as make decisions about individual consumers based on usage profiles. Whilst it is acknowledged that such decisions can often be to the benefit of consumers in terms of energy savings, it is also emerging that there is potential for intrusion into the private lives of citizens through the use of devices which are installed in homes. It also marks a shift

---

<sup>1</sup> Smart meters: controlling your energy bill? *Euractiv.com*, [online] Available at: <http://www.euractiv.com/en/energy-efficiency/smart-meters-controlling-your-energy-bill-links-dossier-257199> [Available 25 March 2011]  
This article refers to the milestones featuring in The Third Energy Package, adopted June 2009.

in our fundamental relationship with energy suppliers in that consumers have traditionally simply paid suppliers for the electricity and gas that has been supplied. With the advent of smart meters, the process is more complex in that the data subject will provide suppliers with insights into personal routines.

The widely discussed benefits of smart energy use include opportunities for consumers to cut their bills by changing their habits, perhaps using energy at different times to take advantage of lower tariffs, as well as opportunities for industry to more accurately forecast demand, reducing expensive electricity storage costs. The realisation of climate change targets relies to some extent on consumers releasing personal data, but this needs to be achieved in such a way that all parties involved in programmes to introduce smart meters and the development of the smart grid ensure that the fundamental rights of individuals are protected and respected. Without such 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. Such rejection may arise even if there is no breach of the law. In short, from a data protection point of view, the Article 29 Working Party would emphasise that while the potential benefits of these programmes are far-reaching and significant, they also have the potential to process increasing amounts of personal data, unprecedented in this industry, and to make that personal data more readily available to a wider circle of recipients than at present.

The Working Party is aware that there is a huge variation in circumstances between member states, ranging from those where rollout is largely complete following government mandate to those where no meters have been installed.

There is also much variation in the level of involvement from DPAs. Where it is not already the case, the Working Party would remind all involved in smart metering of the importance of consultation with the relevant DPA.

Further differences can be found in the nature of the market across member states, and where responsibility lies with installation of meters. In a number of member states, publicly owned utility companies are responsible. Elsewhere, there is a competitive

supplier market. Distribution system operators have a more prominent role in some countries. In some member states, the replacement of the meters is mandatory for every customer. When the meter register is sent to the DSO, the energy suppliers may have the right to access the information they need in order to manage their customers and issue their bills. They can also access more detailed information (for example in order to give advice about energy savings), but only with customer consent. The DSO has also the right to collect detailed information about their customers' consumption, in order to manage and maintain its physical network.

There are also multiple and complex methods of communication, with additional entry points and data paths creating complicated security challenges requiring solutions that encompass them all.

Given the complex and disparate landscape, the task of producing recommendations is potentially challenging, and at this stage it seems that they can only be general, rather than specific. Therefore it seems sensible and realistic at this stage to set out clear terms of reference for this analysis, focussing on the relationship between the legal requirements set out in the Data Protection Directive and the context of smart metering. As appropriate, it will refer to the research that has been carried out already by the Smart Grids Expert Group<sup>2</sup>. For example, the messages in this opinion about Privacy by Design and security coincide with recommendations made by the Group. What is inarguable is that mass rollout of smart meters is already happening, so there is urgency for us to collectively understand the way that smart meters process personal data, and the issues that this raises, even if the scope of this piece of work is not exhaustive.

---

<sup>2</sup> To facilitate and support the process of an EU-wide Smart Grid implementation, the European Commission decided to set up a Task Force on Smart Grids. To this end, three expert groups were established to identify recommendations for the implementation of Smart Grids. The document used to inform this opinion is:  
Task Force Smart Grids Expert Group 2, *Regulatory Recommendations for Data Safety, Data Handling and Data Protection Report Issued February 16 2011*, [online] Available at: <  
[http://ec.europa.eu/energy/gas\\_electricity/smartgrids/doc/expert\\_group2.pdf](http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf)> [Accessed 25 March 2011]

The opinion seeks to address the following issues: the definition of personal data in the context of smart metering, data controllership and reviewing legitimate grounds for processing. Recommendations made here will be based on current knowledge, but it is likely that future work will be necessary to address future issues (eg smart appliances).

## **Definitions**

A variety of definitions of smart meters and smart grid have been available. However, in order to embrace the issues and priorities identified by the Article 29 Working Party, it is a useful exercise to define the smart grid and smart meters in this way:

Smart meters are installed in the homes of utility consumers, and are capable of two-way communication. They inform consumers about the amount of energy they are consuming, and this information can also be sent to energy suppliers, and other nominated parties. The key feature of smart meters is that they provide the ability for these remote communications between the meter and authorised parties such as suppliers, network operators, and authorised third parties or energy service companies. Smart meters can increase the frequency of communication between the consumer and the other parties and as a result increases the amount of data about the consumer which is available to those other parties. The collection and use of data is much wider and for a larger number of purposes than traditional or ‘dumb’ meters which are physically read on a relatively infrequent basis.

In the most abstract and basic terms the smart meter takes a reading which reflects the energy usage at the property. At some point that reading, along with other information, can be transmitted outside the property. In some models it will be sent directly to a central communications hub where the smart meter data are managed. Once there, it can be accessed by DSOs, suppliers and ESCOs.

The implementation of smart meters is a pre-requisite for the smart grid. The *Smart grid* is an intelligent electricity network that combines information from users of that grid in order to plan the supply of electricity more effectively and economically than was possible in the pre-smart environment.

## **Application of data protection law to the processing of data collected via smart meters**

Where personal data are contained in the information generated and disseminated by a smart meter, the Working Party determines that Directive 95/46/EC applies to such processing.

From the general information available on this subject and from detailed discussions at national level with regard to the operation of smart meters, it has been established that the following data types can be assumed to be processed:

- Unique smart meter ID and/or unique property reference number (even in the absence of these identifiers, the meter might also be identified by its unique energy load graph);
- Metadata referring to the configuration of the smart meter;
- A description of the message being transmitted, for example whether it is a meter reading or a tampering alert;
- A date and time stamp;
- Message content.

Message content is likely to include the following types of information:

- Meter register read. This could be a single reading or a group of readings for a more complex tariff;
- Alerts. The meter may transmit a message informing that an event has triggered the meter's alarm;
- Network level information such as voltages, power outages and power quality;
- Load graphics with various levels of detail.

Data can be sent to the controller in real-time or be stored in the smart meter. In both cases however, under the Data Protection Directive, it is considered that the data have been collected by the controller.

This list is far from exhaustive but the Working Party notes that the operation of smart meters – and by extension any further developments of smart grids and appliances – entail the processing of personal data as defined by Article 2 of Directive 95/46/EC



and interpreted by the Working Party in its opinion 4/2007. Furthermore, the increased amount of personal data being processed, the possibility of remote management of connection and the likelihood of energy profiling based on the detailed meter readings make it imperative that proper consideration is given to individuals' fundamental rights to privacy.

The conclusion that personal data are processed has been reached for the following reasons:

1. the data enumerated above as being generated by smart meters is in most cases associated with unique identifiers such as a meter identification number. For domestic consumers of energy suppliers, this identifier is inextricably linked with the living individual who is responsible for the account. In other words, the device enables that individual to be singled out from other consumers;
2. further, the information collected in the context of a smart metering service relates to a consumer's energy profile in the context of their energy use and it is used to take decisions directly affecting that individual. Most obviously such a decision would be to determine the level of any charges for energy supply but it is not limited to billing purposes;
3. this view is further confirmed if one takes into account the widely promoted benefits of smart meter implementation such as the reduction of overall energy consumption in member states. Clearly, such an objective can only be achieved insofar as the energy consumption of individual consumers is also reduced and, according to energy suppliers and networks, achieving this objective is to a large extent dependent on the collection of large amounts of information about the behaviour of these consumers.

### **The definition of data controller as it applies to smart meters**

It is established that the Directive 95/46/EC places obligations on the data controller with regard to their processing of personal data. Before setting out how those obligations apply in the context of this opinion, it is important for the Working Party to set out its view on which legal persons fall under the definition of data controller.

Smart meter implementation involves a number of organisations in the processing of personal data potentially including, but not limited to, energy suppliers, energy network operators, regulatory bodies, government bodies, third party service providers and communications providers. Given the number and complexity of relationships, it is likely that there will be difficulties in applying the relevant definitions but the analysis in this Opinion reflects the approach taken by the Working Party in its Opinion 1/2010 on the concepts of data controller and data processor. Therefore, the responsibilities stemming from data protection legislation should be clearly allocated in such a way that compliance with the data protection rules will be sufficiently ensured in practice.

### **Energy suppliers**

In some Member States, the legal person with the most responsibility for processing personal data would be the supplier. They have the contract with the data subject which initiates the processing and by deciding which data they require to fulfil their functions and how they will collect, store and use the data, they can obviously be said to have determined the purposes for which, and the manner in which, the personal data are processed. This establishes them quite clearly as a data controller for the processing of personal data generated by an energy meter and the Working Party is of the view that, notwithstanding the added complexities brought about by smart meters, suppliers remain a data controller in this context.

### **Network Operators or DSOs**

In other models, the DSO which owns the grid will be responsible for the installation and running of the Smart Meter system. The DSO will also be responsible for determining how the data are collected, stored and used. In this model the DSO will be a data controller. Where the energy suppliers have the right to access the data transmitted by the meters and are using the data for their own purposes (for example, to issue bills or to give advice to consumers) then they will also be a data controller for the personal data they are processing.

### **Other parties**

There are many other parties who could potentially be processing personal data in the course of fulfilling their role in a programme to implement smart meters. Some of them may not even come into existence until the full effects of the shift towards greater amounts of personal data processing are apparent so it would not be prudent to attempt a definitive list at this stage. It is also relevant to remember the variations in supply models and concepts across member states. However, it is important to recognise that without all parties operating on a shared understanding of how the definition of data controller applies there is an increased risk that compliance and good practice will not be achieved. With this in mind the Working Party would remind all parties of the following important points:

1. In some implementation models a central communications function is established which has responsibility for managing the transmission of data between the meter and the supplier. It is possible that this function could exist as a data processor acting only on the instructions of the suppliers to and from whom it sends and receives data. However, if in any case the communications function is engaged in deciding whether personal data can be disclosed to a third party, or whether such data can be processed for new purposes, then the communications function could assume the role of data controller in respect of that personal data processing.
2. Energy Regulators are also important actors. They may have access to data for policy setting and research purposes. Insofar as those data are personal data then clearly the regulatory body will assume the role of a data controller.
3. Third party service providers (often referred to as Energy Service Companies or ESCOs) will have an increasingly prominent role in the use of data generated by smart meters. Where personal data are disclosed to the ESCO in order for them to provide a service either to the consumer or to another party, such as a supplier, then the ESCO will assume the role of a data controller.

### **Lawfulness of processing and legitimate grounds/purposes for processing**

Once it has been established that a legal person is to be considered as a data controller, it is then important to set out the legal requirements placed on the data controller by the Data Protection Directive. In accordance with Article 6 of the Directive, personal data must be processed fairly and lawfully. For any personal data processing to be lawful it needs to satisfy one or more of the six grounds for legitimate processing set out in Article 7 of the Directive.

The Working Party notes that in many, if not all, member states the exact nature of the purposes for the processing of personal data stored on or transmitted by a smart meter has yet to be made absolutely clear or properly defined. In light of this, the Working Party would advise that such purposes need to be established before any claim that the grounds for processing are legitimate can be made. The Working Party also notes that each separate purpose has to be, in and of itself, legitimate and that one legitimate purpose cannot serve to further legitimise any other. Specifically, personal data cannot be reprocessed for another purpose which is incompatible with the purpose for which they were originally collected.

The Working Party's view is that there are five possible grounds for processing available to data controllers in this context.

## **Consent**

It is clear that many of the purposes for which personal data may be used will relate to enhanced services offered to the data subject, such as time of use tariffs or energy advice. Where a data subject has agreed to accept such a service, it is likely that the service provider – either a supplier or a third party – will have the opportunity to gain the consent of the data subject for the processing of personal data.

The Working Party would remind data controllers that reliance on consent will require consideration of the fact that valid consent only exists when the data subject has made a fully-informed decision. It is not possible to use consent as a grounds for processing personal data unless the data subject has been given sufficient information about the personal data processing to make a genuine choice. In particular, where there are a

number of different functionalities, then the consent should be granular enough to reflect these multiple purposes rather than one consent being used to legitimise possibly divergent and unrelated different purposes.

The Working Party would recommend that industry develops effective and practical means by which data subjects can express their consent. It is important to remember that consent has to be freely given and must therefore be capable of being revoked so the methods for gaining consent should build in the capability for the data subject to change his mind without going to excessive amounts of trouble. One possible solution could be to design the household control panel to include 'push button' consent. The availability of this type of functionality would depend on the sophistication of the design of the meter and control panel in order to ensure that the process of consent remains valid.

## **Contract**

Processing may also be necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of a data subject prior to entering into a contract. This legal basis could be used to legitimise the processing of personal data for the purpose of billing as without an accurately compiled bill, the contract to supply energy cannot be fulfilled.

In respect of billing, it is important to remember the element of necessity in this condition. In other words, if the grounds for processing are for the performance of a contract that only requires the customer to be provided with and pay a quarterly bill, it is not necessary for the supplier to collect more frequent readings in order to fulfil that contract. Either the contract would need to include valid and legal provision for more frequent readings or the supplier would need to rely on another legal basis for those readings.

## **Performance of a task carried out in the public interest or in the exercise of official authority**

In some member states, the network electricity operator is responsible for the performance of the physical network, but also for reducing the global electricity consumption. This electricity consumption concerns both the global electricity consumption, and the consumption during the peak hours. Those tasks are carried out in the public interest, and they legitimise the installation of the smart meters.

### **Legal obligation**

In some member states, the network operator has the obligation of installing and collecting data through the smart meters for every new installation<sup>3</sup>.

---

<sup>3</sup> See the French decree n° 2010-1022 of August 31, 2010.

## **Legitimate interests**

According to Article 7(f) of the Directive, the processing could be lawful if it is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the personal data are disclosed except where such interests are overridden by the interests or fundamental rights of the data subject.

The key point to be made here is that reliance on this legal basis depends on giving proper weight to the interests and rights of data subjects. It might seem inarguable that the legitimate interests of the data controller and society as a whole would be served by increased efficiency in energy supply and consumption and that this might be achieved via the personal data collected from smart meters. However, simply because this particular use of personal data seems legitimate (and, to many people, desirable) does not mean that it can be applied to legitimise every element of processing. In other words, the imperative to reduce energy consumption, although it might be a sensible public policy objective, does not override data subjects' rights and interests in every case.

Indeed, it is clear that including practical measures such as Privacy Enhancing Technologies and Privacy Impact Assessments to enhance the security and privacy of the data processed by smart meters will make it more likely that this condition for processing could be available to a data controller.

This is particularly important where processing for a data controller's legitimate interests is both inherently and disproportionately intrusive or where the effect of the processing is to cause unwarranted detriment to the data subject. Examples might include the creation of detailed profiles of data subjects that are, in fact, not needed to achieve the purpose, passing details to third parties without the knowledge or consent of the data subject, or the use of personal data to take decisions about remote disconnection without proper regard for an individual's data protection and other rights.

The Working Party would also remind industry that in some member states the possibility for the data subject to object to installation of the smart meter exists and that in such cases the data subject's preferences override any other interests.

### **Further compliance issues raised by smart metering**

Because of the wide ranging nature of the issues presented by smart metering, it is not possible for the Working Party to provide an exhaustive list of points about which guidance could be provided. Indeed, this is an emerging area of work and the Working Party would fully expect that new data protection problems and solutions will evolve as more smart meters are installed. However, there are some issues of general concern which the Working Party believes warrant serious consideration by all those involved in this area.



## **Privacy by Design**

The Working Party recalls its opinion 168 in which it was stated that services and technologies which rely on the processing of personal data should be designed with privacy by default settings. In this respect, smart metering implementation should take place with privacy built in at the start, not just in terms of security measures, but also in terms of minimising the amount of personal data processed. Some member states have proceeded with implementation plans which require a Privacy Impact Assessment and the Working Party would recommend this approach.

The smart meters currently being tested in some member states collect several readings, depending on the type of contract to which the customer has subscribed. For example, if the customer has a simple contract in which he pays the same price for electricity throughout the day, the meter will collect a daily single reading. Alternatively, if the customer has a contract for which there are different prices depending on the time of day, the meter will be collecting ten different readings every day. At its most basic level, Privacy By Design would ensure that meter readings are only transmitted as frequently as necessary for the operation of the system or the provision of a service the consumer has agreed to receive.

For example, one type of meter currently in use collects real time consumption readings every 10 to 60 minutes for the purpose of creating a load graph. The frequency can be adjusted remotely by the network electricity operator. This load graph is stored inside the meter, with a 2 month history, and is collected by the electricity network operator whenever it is needed. Adopting the privacy by design approach, this model could be adjusted in order to collect and store the load graph only on request.

The technical specifications of the network should also ensure that any data collected should remain within the household network unless transmitting it elsewhere is necessary, or if the data subject consents to the transmission. Also, the system should be designed to ensure that even where personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are filtered

out or removed. The overall aim should be that the lowest possible data volumes are processed and transmitted.

The Working Party also recommends that systems are designed so as to allow access to personal data only to the extent necessary for the role being performed by the data controller. All parties who are accessing personal data should be verified as being appropriate and competent recipients of the personal data and they should only be capable of accessing personal data necessary for them to fulfil their role. They should not have access to personal data beyond this scope.

### **Retention of personal data**

In the 'pre-smart' world, the energy industry has developed practices for the retention of personal data for a limited number of purposes, for example, billing. The smart metering environment presents new challenges. Given that substantially greater quantities of data will be processed, retention policies and practices will need to be established for new purposes and reviewed for existing purposes. In order to be certain that data is being retained only as long as necessary to achieve a specified and lawful purpose, then a clearer understanding of the purposes of processing must be established. This in turn will enable controllers to demonstrate that personal data is only being retained for as long as necessary. For example, one purpose mentioned quite frequently is that the data collected from a meter would allow for the provision of energy efficiency advice. In some cases this type of service might include offering year on year comparisons and it has been suggested that thirteen months may be an appropriate time period for retaining personal data in order to satisfy this purpose. However, such a long retention period would only be acceptable where the data subject has agreed that they would take advantage of such a scheme. For the provision of other types of service a much shorter retention period should be required.

Furthermore, it is conceivable that consumers could hold much of this data on the meter or comparable gateway device (other than that required for billing purposes). This gives the opportunity to allow the data subject to make their own decisions regarding retention. If this were the case it would be advisable for consumers to receive a system of prompts or reminders to assist with this housekeeping.

### **Third Parties' processing of personal data**

It is likely that there will be significant involvement of third parties/ESCOs delivering and supporting the smart metering implementation and the Working Party believes this will require careful consideration. The influence and involvement of third parties will vary from member state to member state but it is clear that at its most intrusive the implementation of smart metering could result in a trade in energy profiles in the interests of those parties wishing to market energy services.

Techniques that have been suggested to assist with compliance include establishing a central information and communications hub which acts as a conduit for all those involved who wish to access consumer data; a Code to which all parties must be signatories; and a Charter which would span the whole industry. The Working Party wishes to make it clear that the more intrusive the processing, the more rigorous the safeguards need to be. The Working Party would strongly urge relevant regulatory bodies to take a view on the acceptability of the more intrusive processing.

Underpinning all of these would be consumer consent, with the industry ensuring that the data subject is in a position to grant this in an informed way. The Working Party wishes to make it clear that it would be unacceptable for third parties to be processing detailed information about a data subject's energy usage without the knowledge and consent of that data subject.

### **Security**

As part of the Privacy by Design process, security and privacy risk assessments will identify the potential risks to data security. Given the novel and vast prospect that is in store with the smart grid and its associated technologies, the task of anticipating security requirements is a challenging one.

Bearing this in mind, this Opinion recommends that in order to mitigate risk, the approach should be end-to-end, incorporating all parties and drawing on a broad range

of expertise. Security should also be designed in at the early stage as part of the architecture of the network rather than added on later.

The Working Party wishes to make it clear that for data subjects to be confident that their personal data are processed securely and their fundamental right to privacy protected, appropriately robust security safeguards must be in place. These safeguards should apply to the whole process including the in-home elements of the network, the transmission of personal data across the network and the storage and processing of personal data by suppliers, networks and other data controllers.

The Working Party anticipates that smart meters will have a long life expectancy and therefore advises that safeguards will need to be updated and improved over time and must be regularly subject to review and testing.

Given the increased amounts of personal data being processed it is clear that the risk to data privacy also increases. Therefore, the Working Party recommends that technical and organisational safeguards should cover at least the following areas:

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

### **Individual rights including information provided to data subjects.**

The implementation of smart meters will give rise to complex and novel personal data processing operations. Most data subjects will be unaware of the nature of these

operations and the potential impact this could have on their privacy. Certainly, if they are not aware of the personal data processing then it is impossible for them to make informed decisions about it. The obligation to inform data subjects about the processing of their personal data is one of the fundamental principles of the Data Protection Directive. Article 10 regulates the provision of this information and requires data controller to make the following information available to the data subject:

- The identity of the data controller and of his representative if any;
- The purposes of the processing;
- Any further relevant information which would render the processing fair. This includes the identity of the recipients of the personal data, the existence of the rights of access and rectification.

The data controller responsible for the installation and maintenance of the meter should make clear to data subjects what information is collected from the meter and what it is used for.

Insofar as third parties are involved in the processing of personal data for the purpose of providing services to data subjects, data subjects should be similarly informed. In some circumstances, it might be appropriate to allow for independent vetting or monitoring of third party access to and use of personal data to ensure that data subjects are not being misled.

### **Rights of the data subject**

Data controllers must respect the rights of data subjects to access and, where appropriate, to correct or delete information held about them. Clearly, the fact that an integral part of the smart metering project is the implementation of a 'home network' (where the consumer can obtain instant information from the smart meter about their usage patterns and tariffs), means that there is an opportunity to ensure that data subjects are able to exercise their rights easily using tools that enable direct access to data.

However, some of the technology may not be able to facilitate subject access to their data. For example, one of the meters currently being tested in some member states has only a small text-only display. This will neither allow the customer to access the information already transmitted by the meter, nor the display graphics, such as the load graph (which is stored inside the meter). Therefore this display does not seem sufficient to be used for a subject access request.

### **Processing of data for crime prevention and investigation.**

The Data Protection Directive regulates against the processing of personal data where the processing is excessive with regard to the purpose. It is clear that the detailed picture obtained by smart meters that inform suppliers about patterns of energy use might allow for the identification of suspicious and, in some cases, illegal activities. The Working Party would remind the industry that the fact that such a possibility exists does not automatically legitimise wide scale processing of data for this purpose. It is particularly important to note that insofar as personal data relates to the alleged committing of an offence, that this personal data would be categorised as being sensitive and, as a result, the data controller cannot process such data unless Article 8 (5) of the Directive applies.

### **Conclusion**

The arrival of smart metering, which paves the way for the smart grid, brings with it an entirely new and complex model of inter-relationships which poses challenges for the application of data protection law. Responses to the Directorate-General Energy questionnaire demonstrated that there is much diversity in the position across EU Member States, both in terms of progress of the implementation, and energy supply arrangements which further complicates the scenario. However, what is abundantly clear is that smart metering is enormous in scale: it is projected that the vast majority of European citizens will have one installed in their homes before the end of this decade.

This opinion explains the applicability of data protection law: it has demonstrated that personal data is being processed by the meters, so data protection laws apply.

This opinion has shown that smart metering brings with it the potential for numerous novel ways for processing data and delivering services to consumers. Whatever the processing, whether it is similar to that which existed in the pre-smart environment, or unprecedented, the data controller must be clearly identified, and be clear about obligations arising from data protection legislation including Privacy by Design, security and the rights of the data subject. Data subjects must be properly informed about how their data is being processed, and be aware of the fundamental differences in the way that their data is being processed so that when they give their consent it is valid.

Done at Brussels, on 4 April 2011

*For the Working Party*

*The Chairman*

*Jacob KOHNSTAMM*