Smart metering under EU data protection law

Rainer Knyrim* and Gerald Trieb**

Abstract

- Smart metering systems require an early awareness of their massive implications with data protection and privacy issues. Consideration from the outset enables the development of special architectures designed for privacy, which may decisively reduce privacy risks.
- The requirement for the obligatory consent of consumers to the installation of smart meters should be avoided, since it threatens the goals—improvements in energy and cost efficiency as well as consumer information—of the new technology.
- The collection and processing of the detailed consumption data of consumers could be based on various other legal foundations, of which the existence of a specific and valid legal obligation is the most favourable and firmly based as far as it reasonably balances the needs of the utility providers and the privacy rights of the consumers.
- Consumer's privacy rights may not be overridden, since their positive acceptance of and active use and involvement in the new technology are key concerns and parameters for achieving its very creditable goals.

Introduction

So-called 'smart metering' refers to a new generation of advanced and intelligent metering devices which have the ability to record the energy consumption of a particular measuring point in intervals of fifteen minutes or even less. These so called 'smart meters' can also communicate and transfer the information recorded in real time or at least on a daily basis by means of any communications network to the utility company for purposes such as monitoring of the system load as well as for billing purposes ('tele-metering').

In addition to the ability to measure the consumption over very short intervals, smart meters enable a two-way communication between the meter and the central system of the utility company, the so called distribution systems operator (DSO). In other words, a smart meter not only communicates current or recent metering data, but it also enables the DSO—and possibly the energy supplier as well–to remotely control functionalities of the meter. Thereby, the meter could be easily switched off and at the same time cut off the household or business entity connected to the particular meter from the delivery of energy.

Nowadays, when talking about a smart meter, one usually refers to a meter measuring the consumption of electric energy, although the term should also become very common for respective devices measuring the consumption of natural gas and water. For the purposes of this article, the term 'smart meter' refers to an intelligent measuring device which has the ability to either meter the consumption of electric energy or natural gas at a certain, specific measuring point.

Data protection and data security implications of smart metering

Dangerous information: 'Metering Data'

Smart meters may theoretically provide the recipient of the measuring data with real time information on the energy (electricity) consumption of the measuring point. The recording of measuring data in intervals of 15 minutes is currently being discussed at the European level, as well as in many of the Member States. From such detailed metering data precise graphs of the actual consumption can be easily drawn up. A simple interpretation of such a graph may reveal much information on the behaviour and daily habits of those persons or households from whom the metering data

* Dr Rainer Knyrim is Partner, Preslmayr Attorney-at-Law, Vienna, knyrim@preslmayr.at.

** Dr Gerald Trieb is Associate, Preslmayr Attorneys-at-Law, Vienna, trieb@preslmayr.at.

derive. This information may include, for example, the time those persons get up in the morning, have their breakfast, leave their house or flat for work, return home, and go to bed. An expert may even be able to obtain information on which electronic devices (such as a toaster, a TV set, a laundry machine, etc.) those persons use.

The availability of such information leads to the danger that people's behaviour and habits may be controlled and monitored by third persons. Third persons, moreover, may have a particular interest in the data: advertising companies might use them for specific behavioural advertising campaigns, litigants may use them in civil lawsuits, and a landlord could use them to prove whether or not the tenant does or does not have a pressing need for accommodation (which, under certain circumstances, might be a requirement for the right to obtain a publicly rented flat). Furthermore, fiscal authorities could take advantage of accurate and detailed metering data to prove, for example, whether a house or a flat is used as a principle residence by the taxpayer or not.

Data security risks

Besides issues of material data protection law, the risks with regard to data security are considerable. Due to the high value of detailed metering data, cyber attacks by private third parties as well as by foreign governmental agencies are to be expected. Furthermore, since smart meters can be remotely controlled via the network, the system might also become a preferred target for terrorist attacks in the form of switching off whole areas from electricity or other energy sources. Therefore, compliance with data security regulations is essential when designing smart metering systems. However, due to the high inconsistency of the implementation of the security requirements among the Member States and the lack of an international standard, maintaining data security within a smart metering system will become a tough challenge for an internationally operating grid provider.

Assessment of compliance

Due to the widespread implications of the implementation and operation of the new metering technology, a stringent and intense evaluation of its compliance with data protection principles and regulations is necessary. Such evaluation has to initially assess whether the processing of the metering data by the data controller can be performed in accordance with data protection regulations. In another step, possible legal bases for a transfer of the metering data have to be analysed. Moreover, its compliance with core principles of the law such as data minimization, legitimate data processing, transfer only for specific purposes, and data storage being no longer than absolutely necessary for such purposes has to be examined as well.

Accordingly, legislative bodies of countries which are in the course of implementing the new technology should devote attention to the privacy issues connected to smart metering and not ignore or overlook its interferences, infringements, and dangers with respect to data privacy rights. The initial implementation efforts taken in the Netherlands impressively demonstrate that privacy implications of smart metering should be seriously taken into account from the very beginning of the implementation process. If such issues remain unsolved or even ignored by lawmakers, then the implementation process might be suddenly stopped and sent back to the beginning.

This is exactly what happened in the Netherlands, where the current, completely modified draft of the implementation package is the outcome of protests by consumer associations; as a result, the implementation was changed to provide consumers with the right to refuse installation of a smart meter. This concept, on the one hand, reflects legitimate consumer interests, but, on the other hand, makes it more difficult for the DSOs to realize the purposes and goals of the new technology, which are namely the improvement of energy efficiency, grid quality, and stability as well as customer information. A successful macro-economic implementation, indeed, is depending on the installation of the new technology at the vast majority of the measuring points.

Despite the model of the Netherlands, a privacy friendly implementation of smart metering does not necessarily have to require the explicit consent of every consumer to the installation of a smart meter, as other legal bases provided for by European data protection legislation are available, as discussed in detail below.

The European legal framework

For purposes of assessing the legal provisions covering the implementation of Smart Metering, three different regulations have to be considered. Those are, first, the European Convention on Human Rights, secondly, the Third Legislative Package in the energy sector of the European Union as well as the third Data Protection Directive.

Article 8 of the European Human Rights Convention

Article 8(1) of the European Convention on Human Rights (ECHR) [Convention for the Protection of Human Rights and Fundamental Freedoms] provides everyone with a right to respect for one's 'private and family life, his home and his correspondence'. However, this guarantee is subject to certain restrictions which must be 'in accordance with law' and 'necessary in a democratic society' (ECHR Article 8(2)). The European Court of Human Rights has interpreted these provisions to develop a right to data protection and a catalogue of requirements by which to measure applicable national legislation.

Third Legislative Package

In 2009, the European Union enacted two directives as part of the 'third legislative package', one which sets forth common rules for the internal market in electricity ('Electricity Directive'),[1] and the other which deals with the internal market in natural gas ('Natural Gas Directive').[2]

These directives recommend the implementation of intelligent metering systems, which may be subject to an economic assessment of the long-term costs and benefits to the markets and the individual consumer. This assessment should be finalized no later than 3 September 2012. In case the results of the economic assessment are positive, paragraph 2 of Annex 1 of the Electricity Directive stipulates that at least 80 per cent of consumers shall be equipped with smart meters by the year 2020. A similar provision has also been enacted for the implementation of smart meters for measuring the consumption of natural gas.[3] However, since the technology of natural gas meters is not as highly developed as that for smart electricity meters, the Natural Gas Directive does not include any specific deadline for the implementation of smart metering in the natural gas sector.

Closely connected to the implementation of smart metering systems are provisions included in Annex 1, para. 1 of the Electricity Directive which provide that consumers shall have their consumption data at their own disposal within a sufficient timeframe. Furthermore, they shall be able by explicit agreement and free of charge to give any registered supply undertaking access to its metering data, as well as be properly informed of their actual electricity consumption and its costs, which shall be ensured frequently enough in order to enable them to actively regulate their own electricity consumption and use energy move efficiently. Those provisions shall promote the development of a new branch within the energy sector, namely the provision of so called 'Value Added Services' (VAS).

Data Protection Directive

According to Article 2(a) of the EU Data Protection Directive ('Data Protection Directive'),[4] '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, psychological, mental, economic, cultural or social identity.' Both because the Directive's definition of personal data is to be broadly interpreted, and because some national data protection laws of the Member States refer in their definition of personal data to those belonging to a 'community of persons' the data are related to,[5] the metering data can be considered to be personal data. Therefore, the provisions of the Data Protection Directive are applicable even if more than one person lives in a household equipped with a smart meter.

Legal processing of the metering data

According to Article 6 of the Data Protection Directive, personal data must be processed fairly and lawfully, collected for specific and legitimate purposes and may not be further processed in a way incompatible with those purposes. In addition, data processing must be adequate, relevant, and not excessive in relation to the purposes for which the data are collected. With respect to smart metering, the processing may be based on various purposes such as the improvement of energy efficiency, metering accuracy, customer information, grid stability, as well as timely billing. Therefore, the data collected by smart meters could be legitimately processed for different purposes and, as a consequence,

1 Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, [2009] L211/55.

2 Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, [2009] L211/94.

3 Natural Gas Directive, Annex 1.

4 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.

5 See, eg, Austrian Datenschutzgesetz 2000, § 4(3).

might be subject to different restrictions of processing and transmission.

The processing of personal data, however, does not only have to comply with the principles mentioned above, but also has to be justified under Article 7 of the Data Protection Directive. According to this provision, processing of personal data may only be legitimate if one of the following conditions is satisfied (listed here in order of apparent suitability for smart metering):

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

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

(c) the data subject has unambiguously given his or her consent; or

(d) processing is necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1) of the Data Protection Directive.

The addressee of the regulations concerning the legitimacy of processing is the controller of the data application. With respect to smart metering, the DSO companies certainly qualify as controllers, since they (as the owners of the meters) determine the purposes and means of the processing of the data; the DSO also implicitly decides which kinds of personal data are collected and are transferred to other parties. Such parties may include energy suppliers, governmental agencies, and other third parties having an interest in the metering data. The lawfulness of the processing and transmission of metering data has to be determined for each type of party that will process the data. We will consider each legal basis in turn.

Processing for compliance with a legal obligation of the controller

The existence of a legal obligation or legal authorization of the data application by statute is generally the most favourable and strongest legal basis for data processing. With respect to the implementation and operation of a smart metering system, no such legislative provision currently exists on the European level. The Electricity Directive itself does not qualify, since it requires implementation by the national laws of the Member States. Therefore, it is currently up to the Member States to provide an explicit legal foundation, which could be included within statutes regulating the national electricity and gas markets.

National statutes mandating the implementation of smart metering have been enacted in some EU Member States (such as in Italy and Sweden). In Austria, the statute only obliges utility companies to ensure delivery of energy at a low price and with high quality. A draft statute regulating the implementation of smart meters and implementing the EU energy directive passed the Austrian parliament in November 2010, but lacks provisions on important issues of data protection, such as the permissible period of storage of the data or a determination of the legitimate interval for measuring the consumption data. Rather, the draft 'passes the ball' to the regulatory agency to enact administrative regulations, which shall set forth the concrete design for smart metering, a procedure which has been criticized with regard to the provisions of Austrian constitutional law.

In order to comply with applicable legal requirements under Article 8 of the European Convention on Human Rights as set forth in the case law of the European Court of Human Rights,[6] any legislation providing a legal basis for the processing of smart metering data would have to meet the following conditions:

- provide an appropriate indication as to the scope and conditions of the data processing;
- provide for a determination of the possible group of data subjects; contain rules for a procedure to be followed;
- regulations prohibiting certain kinds of comments of the personnel of the controller with regard to the data of the data subjects processed;
- regulations with regard to the legitimacy of the storing of information; provide for a regulation concerning the deletion of the data.

Due to these stringent and detailed requirements that statutes must meet, there are a number of difficult problems to be solved for any legislation to avoid being found incompatible with Article 8.

Processing is necessary for the performance of a contract

The processing as well as the transfer of data can also be legitimate if such processing is necessary for the controller to fulfil a duty or obligation set forth within

6 See, eg, *Amman v Switzerland* ECHR 2000-II App no 27798/95).

a contract entered into with the data subject (ie, the energy consumers). The analysis of whether any contractual duties exist which require the processing of smart metering data, however, must be preceded by the clarification that data subjects have usually entered into two or three separate contractual relationships with the various players in the energy supply market. Legitimacy of processing must therefore be analysed individually for any duty or obligation, as well as for each contractual relationship.

Duty of DSO's to maintain grid stability

According to Article 25 of the Electricity Directive, the DSO is responsible for the long-term ability of the system (grid) to meet reasonable demands for the distribution of electricity and for operating and maintaining under economic conditions a secure, reliable, and efficient electricity distribution system with due regard for energy efficiency. This could be seen as a codification of the general contractual duty of a DSO to ensure a high level of grid quality as well as grid stability and security. As European energy demand has been dramatically and consistently rising for years, DSOs could require accurate and prompt metering data in very short intervals in order to improve their ability to react to energy supply shortages by means of the remote 'switch off' function of the smart meters. Therefore, the processing of smart metering data by the data controller DSO could be justified by its necessity for the performance of a contractual duty.

Nonetheless, the processing could only be justified to the extent that metering data are required for the purpose of ensuring grid stability. Furthermore, the question arises whether the metering data thereby necessarily have to be processed in a personalized fashion.

Accurate billing of energy supplies

By means of the implementation of new metering technology, suppliers may offer their customers various types of energy tariffs (eg, so that the bill might not only depend on energy usage, but also on whether consumption takes place during the day-time, night-time, peak or off-peak, etc.). Such new tariff models would require the transfer of detailed metering data to the energy supplier, which needs those data to provide its customers with accurate and timely bills. This does not only represent a core goal of the third energy package of the EU, but also a main contractual duty of the energy supplier towards its customers. Accordingly, it could be argued that the energy supplier may lawfully receive and use the detailed metering data for billing purposes, in case sophisticated tariffs as described above are agreed with the respective customer (which also requires personalized data).

However, the wording of Article 7(b) of the Data Protection Directive, which legitimates data processing only if necessary for the performance of a contract entered into by the controller and the data subject, could conflict with this argumentation. As already stated above, the DSO is the data controller for the smart metering application, so that any processing or transmission of the metering data from the DSO to the energy supplier cannot, at first sight, be subsumed under the fulfilment of a contractual duty.

Nevertheless, it could be argued that Article 7(b) of the Directive should still apply due to a necessarily broad interpretation of this provision as a reaction to the consistent support and promotion of the unbundling of DSOs and energy suppliers by European legislation in the energy sector over the last decade. Since the DSO and the energy supplier have to be legally or at least economically separated and independent even within the same corporate group, Article 7(b) has to be understood to the effect that a transfer of data might also be legitimate on the ground of performance of a contractual duty, if the transfer is necessary for a third party in order to fulfil its contractual duty towards the data subject. In this context, the DSO may even be obliged to transfer the data in order to facilitate the performance of a contract by a third party towards the consumer (the common contractual partner), which could also establish a contractual duty of the DSO itself. If the DSO was not obliged to make this transfer, the data subject would be deprived of the chance to contract with an energy supplier, since without the possibility of obtaining the metering data for purposes of billing the consumer, an energy supplier would be unlikely to enter into a supply contract with the consumer—a result that could not have been intended by the European legislator.

It has to be noted again that the processing as well as the transfer of data on the basis of the performance of a contract is only lawful to the extent absolutely necessary. The type and kind of the particular tariffs, therefore, will determine the intervals of the measuring and collecting of the metering data. In this context, it seems questionable whether metering data in intervals of 15 minutes or less are really required by the energy supplier for billing purposes, since the offering of tariff models which change the rate so frequently are not very likely from a current perspective. However, it is the DSO as the controller of the application that makes the decisions on the timeframe of the intervals metering data are collected. Therefore, a respective balancing

of the needs of the DSO and the needs of the energy supplier seems to be required.

Unambiguous consent of the data subject

Consent as a legal basis for the processing of smart meter data has a number of weaknesses. First of all, the unambiguous consent of the data subject can be revoked at any time without any reason. In addition, the requirements for the legal validity of such consent are quite strict: consent must be freely and explicitly given by the data subject, and must include a description of the data types as well as the purpose for the collecting or transferring of the data. In addition, courts may only recognize consent if it is stated separately within the contract or even signed separately. Finally, if another legal basis exists, obtaining the consent of the data subject might even be counterproductive, since it may lead the data subject to assume that he or she can simply withdraw his or her consent and thereby immediately end the legality of the data processing.

However, if neither a valid legal obligation for the operation of smart metering exists, nor the transfer of any metering data could be securely based on a duty falling within performance of a contract, the option of obtaining the data subject's consent should be seriously considered.

Processing is necessary to pursue the legitimate interests of the controller

A justification for the data processing could also be found in legitimate interests pursued by the data controller. Such legitimate interests could be found in the statutory and the contractual duty of the DSO to ensure and maintain grid stability and thereby protect the grid from major blackouts. Therefore, it could be argued that the processing of the detailed metering data may be based on those legitimate interests of the DSO as controller. However, this argument would not serve as justification for the transfer of the data from the controller to any third party.

However, in order to be recognized, the legitimate interests of the data controller must outweigh the fundamental interests of the data subjects in non-disclosure of their personal data, which results in a high burden to be overcome. Therefore, whether the interests stated prevail over the privacy rights of data subjects would need to be evaluated in each individual case by a DSO, taking into account the particular 'grid needs' of the DSO as well as technical solutions to reduce the impact on the fundamental rights of the data subjects.

Excursion: Transfer of the metering data to Value-Added Service Provides

With regard to Value-Added Services (VAS; providers might be, for example, an energy efficiency consulting company), performance of a contract does not qualify as a valid legal basis. The needs for and the general value of such services are weaker compared with those for the supply of energy itself. Whereas, indeed, the DSO as well as the energy supplier ensure the satisfaction of a primary need of a consumer which is the supply of energy, a VAS-provider—for example one who does energy efficiency consulting—does only fulfil an additional request or goal of the consumer to maximize the savings of his/her energy costs.

Thereby, the services of VAS-providers include—after an analysis of the energy consumption behaviour of the consumer—advice with respect to more efficient use of energy or to the point of time energy is consumed (given that the consumer is offered tariffs, which supply energy at different rates during peak/off-peak times or day/night). Therefore, there is no contractual duty for the controller to provide VAS providers with the detailed metering data. It could be argued, however, that the transfer of metering data to VAS providers is justified by the overwhelming interests of such providers in the metering data. However, as this argument is not particularly strong, VAS providers are well-advised to obtain the explicit consent of the consumer within its general terms of service (if this is sufficient under national data protection law) authorizing the VAS provider to receive the data from the DSO, even if such consent may be revoked by the consumer at any time.

Summing up, as neither the consent of the data subject nor performance with a contractual duty serve as a secure and strong legal basis for processing the metering data, a comprehensive legal obligation at European or national level obliging the DSOs to collect, process, and transfer the detailed metering data of the customers—which takes into account the Case Law of the European Court of Human Rights as well—would be favourable for all players involved. Such an approach by European or national governments would also be appropriate and would be a first step towards the concept of a Smart Metering System which is designed for privacy.

Privacy by design

'Privacy by design' is an approach whereby privacy and data protection compliance is designed into data

applications processing personal data from the very beginning of the conception of a project, rather than being 'bolted on' later. This approach could also be applied to the implementation of smart metering on two different levels.

On the first level, legislative bodies have to enact legislation which is compliant with data protection law. In particular, the requirements developed for such laws by the European Court of Human Rights should be seriously taken into account, and the rights of data subjects provided for in Article 10 of the Data Protection Directive must be secured (eg, rights of information, access to the data processed, and deletion or correction). Legislative requirements for privacy by design could be one way to fulfil these goals.

On the second level, it is the DSOs' task as the data controller to build up their own technical infrastructure as well as technical solutions for a privacy-friendly smart metering system. Thereby, DSOs should not only ensure that only those data necessary for the purposes of the application are collected and processed, but also that data are only personalized if personalization is really required (ie, if anonymous data would not be sufficient). In this respect, metering data solely required for ensuring the quality and stability of the grid could be easily generated and processed anonymously or in aggregated form, whereas only data needed for the billing process might necessarily be personalized. However, even with regard to metering data for billing purposes, privacy friendly solutions are possible. Metering data needed for the calculation of the price of the energy consumption of a particular metering point according to a special tariff could be separated from those data identifying the persons connected to the measuring point, and be combined only when the final price is calculated. Such a method could ensure that the data received from short measuring intervals cannot be matched to the energy consumption of a particular person or household and, at the same time, strengthen the willingness of consumers to accept this new technology.

EU initiatives regarding the implementation of smart metering

According to Article 49 of the Electricity Directive, Member States are obliged to enact the necessary laws, regulations, and administrative provisions by 3 March 2011. With respect to the implementation of smart metering technology, Member States have adopted very different approaches. This inconsistency conflicts with the goal of the European Commission of a harmonized realization of the smart metering roll-out, in order to have compatible systems throughout the Union.

To facilitate and support the process of an EU-wide roll-out of smart metering, the European Commission decided to set up a Task Force on Smart Grids. The goal of the Task Force is to identify and procure a set of regulatory recommendations to ensure EU-wide consistent and fast implementation of smart grids, while achieving all expected services and benefits for users.

The Task Force is divided into three 'Expert Groups' which are to jointly develop a common vision for implementation. The first subgroup is tasked with the evaluation of the necessary functionalities for smart grids. The second one is tasked with a definition of the regulatory recommendations for data safety, data handling, and consumer protection, while the third group is to define the roles and responsibilities of actors involved in the deployment of smart grids. The Task Force has already published its first reports on the initial assessment of the needs and requirements for smart grids, which have been published on the website of the European Commission.[7] The Task Force is currently working on making the recommendations contained in the reports more concrete, and hopes to publish them some time in 2011.

This installation of the Task Force by the European Union should be highly appreciated by the Member States as well as by the energy industry. It is a step in the right direction towards promoting and accelerating EU-wide implementation that is consistent and legally compliant within a reasonable timeframe. Even if—in order to achieve this goal—there is still some work left for the Task Force and the EU Commission, the guidelines set out by the Task Force, both legal and technical, could serve as a valuable basis for implementation efforts in every Member State and, even more, could decisively reduce implementation costs, if adopted by the EU Commission.

Conclusions

The implementation of smart metering is highly dependent on the collection, processing, and transfer of personal data. Therefore, data protection issues play a very important and even decisive role in the successful implementation of smart metering. Hence, the authors

7 <http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm> (last accesssed 20 January 2011).

recommend addressing such issues at the very beginning of the drafting of relevant legislation and of implementing smart metering at the DSO level. From a technical point of view, privacy issues can be reduced by privacy for design, which means already integrating privacy-friendly solutions into technology and business processes.

The analysis of the applicable legal basis for the implementation and the operation of smart metering systems demonstrates that obtaining the consent of data subjects is a serious possibility. However, due to the difficult requirements of the drafting of consent forms and their legal insecurity, not to mention the ability of data subjects to revoke their consent, consent is usually not the most favourable option. Another option is relying on the performance of a contract as the legal basis, but this is only persuasive in the processing of the data by the DSO as data controller, and is weaker with regard to the transfer of the data to energy suppliers, the providers of Value Added Services, and other third parties. The legitimacy of such transfers has to be based, for example, on a broad interpretation of Articles 7(b) and 7(f) of the Data Protection Directive. Nevertheless, taking into account that (according to almost all academic studies carried out so far) the roll-out of new metering technology is economically feasible only if the vast majority of households is furnished with a smart meter, the establishment of a valid legal obligation, either at the European or national level, might serve as the clearest, safest, and most sustainable way of securing successful implementation.

At the same time, consumers have to be trained and informed about the new possibilities offered by smart meters. By means of a remote Internet access or an in-home display showing their recent and current consumption data, consumers may have much greater opportunity to control their energy consumption. The goal is thus to alter consumers' consumption behaviour to a more cautious and efficient consumption and use of energy. In other words, consumers have to be trained and informed to become active consumers with regard to smart meters; the mere deployment of smart meters, unless it is accompanied by appropriate educational measures, will not cause any difference in the costs or efficient use of energy.

In conclusion, the EU itself, as well as the legislative bodies of the Member States, needs to enact sufficiently definite and detailed regulations which balance the needs of the utilities industry and the privacy rights of consumers. If such interests are balanced in a sophisticated way, the valuable and ambitious goals of an EU-wide smart metering structure can be realized in practice. This will require DSOs to set up smart metering systems which conceptually as well as technically (by 'privacy by design') deal with privacy issues. On the other hand, if the data protection rights of consumers are not sufficiently taken into account, then their acceptance of the new technology will be lacking, which could lead to its unsuccessful implementation.

doi:10.1093/idpl/ipr004
Advance Access Publication 1 March 2011