



Opinion of the European Data Protection Supervisor

on the Commission Recommendation on preparations for the roll-out of smart metering systems

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data²,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 9 March 2012, the Commission adopted a Recommendation on preparations for the roll-out of smart metering systems ('the Recommendation').³ The Recommendation was sent to the EDPS for consultation on 19 March 2012.
2. Before the adoption of the Recommendation, the EDPS was given the opportunity to provide informal comments. Some of these comments have been taken into account in the Recommendation. As a result, the data protections safeguards in the Recommendation have been strengthened.

¹ OJ L 281, 23.11.1995, p. 31.

² OJ L 8, 12.1.2001, p. 1.

³ C(2012)1342 final.

3. The EDPS welcomes the fact that the Commission also consulted him formally and that this Opinion is referred to in the preamble of the Recommendation.

1.2. Objectives and background of the Recommendation

4. The objective of the Recommendation is to give guidance to Member States on preparation for the rollout of smart metering systems⁴ in Europe. The rollout is foreseen by 2020 for both the electricity and the gas markets and is subject to an economic assessment of costs and benefits. This assessment is to be carried out by each Member State by 3 September 2012.⁵
5. A significant part of the Recommendation (Section I) is dedicated to data protection. Importantly, the Recommendation calls for the preparation of a template for a data protection impact assessment⁶ ('the Template') and its submission to the Article 29 Data Protection Working Party ('the WP29') for advice within twelve months of the publication of the Recommendation.⁷
6. The first draft of the Template is currently under preparation by Expert Group 2 of the Commission's Task Force on Smart Grids. The Task Force has been established by the Commission prior to the adoption of the Recommendation, to give advice on smart grid issues. One of the subgroups of the Task Force, Expert Group 2, focuses on security and data protection aspects. The group comprises mainly industry representatives (with some representation of civil society and consumer groups).⁸
7. The Commission pursues a 'soft law' approach combining (i) a Commission Recommendation covering data protection among other issues and (ii) further guidance to Member States in the form of a template for a data protection impact assessment, which is to be applied voluntarily by industry participants. The approach is based on the experience gained from the development and revision, following WP29 comments, of the 'Industry Proposal for a Privacy and Data Protection Impact

⁴ For a brief introduction to smart meters and smart grids, please see Section 2.1 below.

⁵ The roll-out and the cost-benefit analysis are required under (i) Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (OJ L 211, 14.08.2009, p. 55), and (ii) Directive 2009/73/EC concerning common rules for the internal market in natural gas (OJ L 211, 14.08.2009, p. 94). The Commission Proposal for a Directive on energy efficiency (COM(2011) 370 final) ('Energy Efficiency Proposal'), currently before the legislators, includes additional provisions on smart metering.

⁶ With regard to data protection impact assessments, it is to be noted that the Commission Proposal for a revised general data protection framework plans to make data protection impact assessments mandatory in some situations and provide further guidance on how such an impact assessment should be carried out. See Article 33 of the Commission proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)11 final). See also paras 200-205 of the 7 March 2012 EDPS Opinion on the data protection reform package, available at http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package;jsessionid=46ACCFDB9005EB950DF9C7D58BDE5377.

⁷ See para 5 of the Recommendation.

⁸ More information on the work of the Task Force and of Expert Group 2 is available on the website of the Task Force at http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm.

Assessment Framework for RFID Applications'.⁹ However, the Commission has not excluded the need for legislative action at national and/or at the European level.¹⁰

1.3. Objectives, main messages and structure of the EDPS Opinion

8. While this EDPS Opinion is adopted in response to the Commission Recommendation, it is not strictly limited to the content of this Recommendation, as there are important data protection aspects of the rollout of smart metering which are not fully addressed in the Recommendation itself. The EDPS also recalls in this context his formal comments on the Energy Efficiency Proposal.¹¹
9. The EDPS Opinion has three main objectives and messages:
 - First, the Opinion evaluates the Recommendation: it welcomes the Recommendation as a first step, highlights its achievements, but also criticises its shortcomings, including its insufficient specificity.
 - Second, while the EDPS regrets that the Recommendation has not provided more specific and more practical guidance on data protection, he considers that some guidance can still be given in the data protection impact assessment Template, which is currently under preparation. Therefore, the Opinion provides a number of targeted recommendations on the Template.
 - Third, the Opinion calls on the Commission to assess whether, beyond the adoption of the Recommendation and the Template, further legislative action is necessary at the EU level and provides a number of targeted recommendations for possible legislative action.
10. In light of these objectives, the Opinion is structured as follows:
 - Section 2 provides a brief introduction to the concepts of smart meters and smart grids and explains the data protection concerns they raise.
 - Section 3 provides general comments on the Commission's approach followed in the Recommendation, discusses the need for further legislative action, and gives recommendations for a possible legislative action.
 - Section 4 outlines some of the key issues that - in the view of the EDPS - should have been addressed more specifically in the Recommendation. Some of these recommendations may also serve to guide national or European legislators when considering further regulatory or legislative action. Others may be addressed in the data protection impact assessment Template to be developed.
 - Section 5 provides a few targeted recommendations on the data protection impact assessment methodology and on the content of the Template to be developed. These should be read in conjunction with Section 4.

⁹ See http://ec.europa.eu/information_society/policy/rfid/documents/info-2011-00068.pdf and http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf.

¹⁰ It is noted that at the present stage no evaluation of the effectiveness of this soft law approach for the field of RFID has been provided, nor is there any generally available information indicating effectiveness of the approach.

¹¹ EDPS Letter of 27 October 2011 to Mr Günther H. Oettinger, Commissioner for Energy on a proposal for a Directive of the European Parliament and of the Council on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2011/11-10-27_Letter_Oettinger_EN.pdf.

2. DATA PROTECTION CONCERNS RAISED BY SMART METERS AND SMART GRIDS

2.1. Smart meters and smart grids: a brief introduction¹²

11. Smart gas and electricity meters are installed in the homes of energy consumers just as traditional gas and electricity meters. A key feature of smart meters is that they can provide data via remote communications between the meter and energy suppliers, network operators, and other third parties. Smart meters also enable more frequent communication between the meter, the energy supplier, and other parties. Instead of less frequent (e.g. annual or quarterly) readings carried out by physical inspection of the meters, as is the case with traditional meters, with smart meters it will be possible to read and record energy consumption much more frequently, for example, every fifteen minutes.¹³ As a result, there is a very significant increase in the amount of energy consumption data, which can become available to the consumer but also to third parties.
12. The implementation of smart meters is considered 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 compared to what was possible in the pre-smart environment.
13. Smart meters, among others, will enable 'demand response' and 'dynamic' or 'time-of-use' pricing for electricity. This is said to be increasingly important with the connection of more and more renewable energy sources to the grid¹⁴. Instead of a single or other simple (e.g. night and day) tariff, dynamic pricing and more complex tariff structures are expected to be introduced to allow 'demand response', in other words, to allow customers to buy electricity at constantly changing prices, thereby cutting demand at peak times, and thus, resulting in a lower need for peak capacity as well as better integration of renewable energy sources¹⁵. In parallel, in the not-so-distant future, households may start using 'smart' devices that use information obtained from smart meters, such as 'smart washing-machines' that will turn on, or an electric vehicle that will be charged, when electricity is cheaper.

2.2. Data protection concerns

14. The Europe-wide rollout of 'smart metering systems' enables massive collection of personal information from European households, thus far unprecedented in the energy sector. The potential intrusiveness of collection is increased by the fact that data are collected, which may infer information about domestic activities: data may track what members of a household do within the privacy of their own homes.

¹² Many different definitions exist for smart metering and smart grids. This introductory description is, in part, abridged from page 4 of Opinion 12/2011 of the Article 29 Data Protection Working Party on smart metering, adopted on 4 April 2011 (WP 183), available at http://idpc.gov.mt/dbfile.aspx/WP_183.pdf. It is provided purely for informational purposes and is without prejudice to the need for a more precise definition of smart metering systems and smart grids in the data protection impact assessment Template to be developed, and/or in any new legislative or regulatory instrument on smart metering and smart grids.

¹³ See Para 42(b) of the Recommendation.

¹⁴ To illustrate: solar and wind energy depends on sunny or windy weather conditions, and dynamic pricing could encourage the demand for electricity to be shifted to periods when solar and wind installations will be working at high capacity.

¹⁵ This may have significant economic effects as peak capacity is one of the most important parameters in network design and a key factor for investment and costs.

15. Smart metering constitutes a radical change compared to previous data collection practices by energy suppliers. Up until now, energy suppliers have read electricity meters relatively infrequently (for example, annually, or every other year), often relying on customers to self-report interim readings (for example, quarterly). On the basis of these readings an energy supplier may have known, for example, that a particular household used a total of 3600 kWh of electricity for a calendar year, or that the electricity consumption for the third quarter of a specific calendar year was 900 kWh.
16. With the installation of smart meters, it will now be possible to collect much more fine grained, detailed data regarding our energy consumption, down to the hour, quarter of an hour, and more. With data at such granularity, those who have access to smart metering data can know when each individual appliance in a household is turned on and off, and can often also identify what specific appliances are used. Smart meters can also provide a detailed breakdown of energy usage over a long period of time, which can show patterns of use.
17. This raises concerns with regard to security, the rights to privacy and the protection of personal data. Among the most basic concerns are fears that regular smart meter readings, unless the security of data is adequately protected, would indicate to criminals when a house is unoccupied. Data can be used to assess whether anyone is at home and when the members of the household are away at work or on vacation.
18. The risks to data protection, however, go further than these most immediate concerns. Indeed, unless adequate safeguards are established to ensure that only authorized third parties may access and process data for clearly specified purposes and in compliance with applicable data protection law, deployment of smart metering may lead to tracking the everyday lives of people in their own homes and building detailed profiles of all individuals based on their domestic activities. With the sheer amount of information that is being amassed by these smart meters, ubiquitous availability of data from other sources, and advances in data mining technology, the potential for extensive data mining is very significant. Patterns can be tracked at the level of individual households but also for many households, taken together, aggregated, and sorted by area, demographics, and so on. Profiles can thus be developed, and then applied back to individual households and individual members of those households.
19. To illustrate, 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 tools 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.
20. These patterns can be very useful for analysing our energy use for energy conservation. However, patterns and profiles can be used for many other purposes, including, perhaps most importantly, for marketing and advertisement. Indeed, information about energy usage can have high commercial value: companies often already know, from tracking order history online, or tracking shop loyalty cards, credit card or bank card use what consumers buy. By analysing smart metering data, data

collected via RFID tags, and utilizing other developing technologies companies are increasingly also able to tell where, when and how consumers use the products. This additional information can then be used for targeted and personalized advertisement. In addition, profiling may also increase the information imbalance between consumers, on the one hand, and energy suppliers or other third parties who wish to market goods and services to the consumers: the more information a consumer discloses about himself, the easier it will be for any party who wishes to sell him a product or service to turn such informational advantage to its own benefit, for example, to engage in price discrimination.

21. Further, law enforcement agencies, tax authorities, insurance companies, landlords, employers, and other third parties may also be interested in personal energy usage information.
22. Considering the risks to data protection, one of the key pre-conditions for the rollout of smart metering systems is to ensure a high level of protection of personal data.

3. GENERAL COMMENTS ON THE APPROACH FOLLOWED IN THE RECOMMENDATION AND THE NEED FOR FURTHER LEGISLATIVE ACTION

3.1. General comments on the approach followed in the Recommendation

23. The EDPS welcomes the efforts made in the Recommendation to provide guidance to Member States on the measures that should be taken in order to ensure that smart metering and smart grid systems are designed and operated subject to adequate data protection safeguards.
24. The EDPS particularly appreciates the efforts of the Commission to make use of newly proposed concepts such as data protection by design and practical tools such as data protection impact assessments and security breach notifications¹⁶. The EDPS also welcomes the references in the Recommendation to data minimization, data protection by default, privacy-enhancing technologies ('PETS's), transparency, and consumer empowerment.
25. The EDPS, in particular, supports the Commission's plan to prepare a template for data protection impact assessment and submit it to the WP29 for advice¹⁷. This approach may help bring consistency and encourage the implementation of the data protection by design principle in the Member States.
26. That being said, the EDPS, in this Opinion, also highlights the issues that in his view would have required more clarity or further specificity in the Recommendation and makes some constructive suggestions as to further steps.

Recommendation and Template should not be read to reduce, in any way, the data protection safeguards established in applicable data protection law

27. Stakeholders must be aware that processing of personal data in the context of smart grids/smart metering will have to fully comply with the national legislation transposing the relevant EU legislation, including Directive 95/46/EC, and - to the

¹⁶ See para 28 of the Recommendation.

¹⁷ As mentioned in para 5 above.

extent applicable – the e-Privacy Directive¹⁸. The Recommendation and the Template may become valuable tools to improve compliance by providing guidance on how to implement data protection safeguards at the practical level. However, they must not be read in isolation and must not be read to reduce, in any way, the data protection safeguards established in applicable data protection law.

28. To illustrate, the first sentence of para 29 of the Recommendation only calls ‘network operators’ to develop and publish an ‘information policy’, under Articles 10 and 11 of Directive 95/46/EC, whereas this obligation, in reality, should apply to all other controllers, including, for example, energy suppliers, operators of smart metering systems, and providers of value-added services. Although the same paragraph uses the term ‘without prejudice to the obligation of data controllers’, it is not clear why this specific obligation is addressed to one particular controller and not to others.
29. Similarly, paras 19 and 20 might suggest that any of the grounds listed in Article 7 of Directive 95/46/EC may be relied on to provide a legitimate legal basis for most data processing in the smart grid or smart metering context, whereas in reality, the choice of legal basis, depending on the specific purposes for which the information will be used, will likely be much more restricted, if Article 7 is interpreted correctly.¹⁹

Data protection concerns should be adequately considered as part of the cost benefit analysis for the roll-out of smart metering systems²⁰

30. The EDPS would have preferred if Section II of the Recommendation had more clearly required a comprehensive data protection impact assessment as an integral part of the cost/benefit analysis. The EDPS would recommend Member States to integrate data protection concerns into the cost-benefit analysis, and the Commission, to make this requirement clearer when following up on the Recommendation.

Need for more specific and pragmatic guidance

31. The EDPS regrets that the Recommendation does not provide sufficiently specific and pragmatic guidance that could be implemented at the practical level and could help ensure a high and consistent level of data protection as well as a level-playing field across Europe.

3.2. The need for further regulatory and/or legislative action at national or European level should be assessed

32. This brings us to a key question: will the Recommendation and the Template be sufficient to ensure a high level of data protection compliance with regard to the deployment of smart metering and smart grid technologies, or will there be further regulatory or legislative action required? If regulation or legislative action is necessary, would purely national actions be sufficient to ensure both a high-level of data protection and a level-playing field for all industry participants across Europe or would legislative action at the European level be warranted?

¹⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.07.2002, p 37), as amended by Directives 2006/24/EC and 2009/136/EC.

¹⁹ See more on the legal basis in Section 4.2 below.

²⁰ See Section II of the Recommendation, which outlines the ‘methodology for the economic assessment of the long-term costs and benefits for the roll-out of the smart metering systems’.

33. Answering these questions requires careful analysis and a well-informed policy decision.

Factors suggesting the need for regulatory or legislative action at national or EU level

34. There are several factors that suggest that specific legislative or regulatory action at national or at the EU-level could be beneficial and/or necessary:

- The supply of electricity and gas are regulated industries currently undergoing very significant changes, which call for adjustments of the regulatory framework. As explained in Section 2 above, until recently only a very small amount of personal data was collected by the meters, which raised limited data protection concerns. Therefore, little or no attention has been paid to providing appropriate data protection safeguards in license conditions or other legislative or regulatory instruments applicable to network operators, suppliers and other market participants. The situation is changing drastically and therefore new safeguards need to be established in these legislative and regulatory instruments.²¹ Such safeguards will be necessary in order to protect the personal data and the interest of consumers, but also, to ensure a level-playing field to all market participants who may wish to have access to the potentially valuable detailed data on energy consumers.
- Directive 95/46/EC does not make data protection impact assessments compulsory. Therefore, although the Recommendation recommends such assessments and although the Commission Proposal for a revised data protection framework proposes to make such assessments mandatory (at least in some circumstances), they are not, at this time, mandatory. Further, even though data protection impact assessments would be mandatory in many cases if the new general data protection framework were to be adopted with its current wording, uncertainties would still exist with regard to the scope of the obligation to carry out such an impact assessment.²²

Factors suggesting the need for legislative action at EU level

35. Additional factors suggest that specific legislative or regulatory action at the EU-level could also be warranted. In particular, it is important to recall that the current data protection framework building on Directive 95/46/EC is not always sufficiently harmonized to ensure a level-playing field to market participants or a consistent level of data protection to individuals whose personal data may be transferred across borders. Neither is it expected that the new general framework for data protection will be sufficiently specific to ensure, in itself, a level-playing field in this specific sector.

36. These concerns may be increasingly important if, as is expected, smart metering and smart grid deployment will lead to innovative new energy services to be offered across borders. To illustrate: if one member State allows its incumbent network operator and/or energy supplier to access detailed consumer data without customer consent and for all purposes, it will be very difficult, if not impossible, for an energy service company based in another Member State to compete, and offer its services across borders, on a level-playing field.

Recommendations for the European legislators

²¹ As will be explained in paras 37-40 below and described in greater detail in Section 4 below.

²² See the Commission proposal for a general data protection framework and the 7 March 2012 EDPS Opinion on the data protection reform package, both cited in footnote 6.

37. In the light of the foregoing, while the EDPS welcomes, as a first step, the adoption of the Recommendation, and encourages the on-going work on the Template, he emphasizes that further reflection is needed to be undertaken as soon as possible on whether further legislative action at the European level may be necessary in the future to further regulate the data protection issues related to smart metering or smart grids. This legislative action, for example, may take the form of specific provisions on data protection in a new Council and Parliament Regulation or Directive on smart grids and smart metering, or an amendment to existing legislative instruments (e.g. Directives 2009/72/EC and 2009/73/EC²³).
38. With regard to the content of such legislation, the EDPS specifically recommends that legislators consider all items outlined in Section 4 below. This should be the case especially (but not only) if the Commission were to introduce additional legislation on the broader aspects of smart metering and smart grids in the near future. In this case, this broader legislative instrument could also be used to comprehensively address all key data protection issues that require specific measures or clarifications.
39. Further, and before more comprehensive legislative action may be taken, as an immediate action point, the EDPS recommends that the Commission and the legislators also consider whether some targeted changes can already be introduced via a modification of the Energy Efficiency Directive, which is currently being discussed within the European Parliament and the Council.
40. In particular, the EDPS recommends including a provision in the Energy Efficiency Directive, requiring controllers to conduct a data protection impact assessment as well as mandatory data breach notification for all controllers processing granular smart metering data (see Section 4.7). He urges Council and Parliament to amend the text of the legislative text currently under scrutiny.

Need for close cooperation between energy regulators and data protection authorities

41. Finally, the EDPS would also encourage energy regulators to work closely with data protection authorities in Member States: considering that the energy sector is already a regulated industry, it appears that a lot can be accomplished by providing specific guidance and establishing at least certain data protection safeguards in license conditions or in other regulatory instruments.²⁴ These measures aiming at a higher level of data protection, can also simultaneously contribute to the accomplishment of other legislative and regulatory goals, such as enhancing consumer confidence, providing a level-playing field allowing fair competition, and encouraging market entry for the provision of energy services. Data protection, thus, ultimately, can make a significant contribution to achieving energy efficiency objectives and climate targets.

4. SPECIFIC COMMENTS ON THE KEY DATA PROTECTION ISSUES RAISED BY SMART METERING AND SMART GRIDS

42. The EDPS, in this Section 4, outlines some of the key data protection issues raised by smart metering and smart grids. In his view these points should each have been specifically addressed in the Recommendation or in a legislative instrument. Although

²³ See para 4 and footnote 5.

²⁴ See, for example, <http://www.decc.gov.uk/assets/decc/11/consultation/smart-metering-imp-prog/4933-data-access-privacy-con-doc-smart-meter.pdf>.

the Recommendation has already been adopted, these points continue to be relevant. In particular, they may now provide guidance for the preparation of the data protection impact assessment Template, as well as for the preparation of further regulatory and legislative action.

4.1. Purposes, nature of the processing and categories of data to be processed

43. In the view of the EDPS, the Recommendation should have contained a clear description of the key processing operations carried out, their purposes and the categories of data that are needed to achieve those purposes. In particular, the EDPS considers that guidance should have:

- covered at least the basic data processing operations such as those needed for billing, energy-efficient maintenance of the grid (forecasting and settlement), and maintenance of security (including prevention of fraud);
- differentiated between objectives that can be achieved by the use of aggregated data relating to multiple households (at a level of aggregation and anonymization that no longer allows re-identification of the data subjects), and objectives, which require the use of personal data relating to individual households; and
- identified criteria to distinguish cases where it is necessary to process the fine-grain meter-readings of individual households from cases where it is sufficient to use data applicable for longer periods (for instance, it will not be necessary for an energy supplier to have access to readings every fifteen minutes for billing purposes if it does not use time-of-use billing tariffs or only differentiates between day and night tariffs).²⁵

4.2. Legal basis

44. The EDPS would have also wished that paras 19 and 20 of the Recommendation had described with greater specificity under which specific conditions the different legal basis will make the processing lawful (consent of data subject, contract, legitimate interest, legal obligation, public interest, etc.). References to existing law (Article 7 of Directive 95/46/EC)²⁶ and the Opinion of the WP29²⁷ are helpful but - in the view of the EDPS - here not sufficient. The EDPS recommends that the Template to be developed, and/or future legislative or regulatory action provide specific guidance/requirements in these regards.

45. The EDPS emphasizes that the current legal basis for deployment of smart metering systems (Directives 2009/72/EC and 2009/73/EC²⁸) in itself is not sufficiently specific to be considered as a 'legal obligation' in the meaning of Article 7(c) of Directive 95/46/EC. To ensure legal certainty, the EDPS therefore recommends that a clear

²⁵On data minimization and frequency of meter readings, see also para 42 on page 12, under heading 'Other methods to consider' and subheading 'Frequency of meter readings'.

²⁶ For ease of reference, Article 7 reads as follows: 'Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; 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) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of 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).

²⁷ See Opinion WP183, referred to in footnote 9 above.

²⁸ See para 4 and footnote 5.

distinction should be made between those objectives on the one hand (i) for which energy usage data can be processed for reasons of public interest (Article 7(e)) or other legitimate interests (Article 7(f)) without customer consent, and on the other hand, (ii) those objectives for which customer consent is required.

46. The EDPS recommends that a freely given, specific, informed and explicit consent must be required for all processing that goes beyond processing required for (i) the provision of energy, (ii) the billing thereof, (iii) detection of fraud consisting of unpaid use of the energy provided, and (iv) preparation of aggregated data necessary for energy-efficient maintenance of the grid (forecasting and settlement).
47. To ensure legal certainty and consistent application and interpretation of these provisions, the EDPS further recommends that the Template and/or applicable legislation also clearly specify that (i) tracking energy use (for purposes other than the basic objectives set forth in paragraph immediately above), (ii) profiling of individuals (except for detection of fraud consisting of unpaid use of the energy provided), (iii) targeted advertisement, (iv) value-added services²⁹, and (v) further transfer of the data for such purposes should each require specific, separate consent.
48. Further, the EDPS recommends that those individuals who do not wish to take advantage of time of-use tariffs or other services based on smart meter functionalities (for privacy reasons, health reasons, or otherwise), should not be required to switch to smart meters. Alternatively, these customers should be given the choice to have a smart meter installed on which 'smart functionalities' including both collection of granular data and remote on/off control are disabled. In any event, as a default setting, in the absence of clear choice (i.e. freely given, specific, informed and explicit consent) by the customer, or other compelling public interest grounds specifically set forth in law, the meters of such customers should neither provide granular readings nor enable a remote on/off control function.³⁰
49. In addition, the EDPS suggests that best practice be collected on the way how consent should be given to ensure that consent will be freely given, specific, explicit, informed, and in line with the Opinion of the WP29 on smart metering, which requires, among others, granularity of consent.³¹
50. Finally, the EDPS would welcome further safeguards with regard to access to smart metering data by law enforcement, tax authorities, other government agencies, insurance companies, employers, and other third parties. The EDPS would recommend, among others, restricting law enforcement access to cases when a judicial warrant, or adequate legal instrument, has been obtained, similar to a search warrant before police may enter and search an individual's home.

²⁹ In this context, it would also be helpful, and increase clarity, if the Template were to provide a definition for the term 'value-added service'.

³⁰ On granularity and choice, see para 54, second bulletpoint ('frequency of meter readings'). See also page 15 of the WP29 Opinion referred above, which reminds that 'in some member states the possibility for the data subject to object to the installation of the smart meter exists and that in such cases the data subject's preferences override any other interests'.

³¹ See top of page 12 of the WP29 Opinion. See also Section 4.6, paras 59-60 of this EDPS Opinion.

4.3. Data minimization: aggregation, sampling, frequency of measurements, and the role of Privacy-Enhancing technologies ('PET's)

51. The principle of data minimisation is only briefly referred to in the Recommendation, in recital 13 and in paras 18 and 23. Similarly, the concept of privacy-enhancing technologies is only briefly mentioned in recital 13. The EDPS recommends that these essential principles and concepts be addressed in a more specific manner - for the moment, at least in the Template - as they represent key solutions to many of the data protection issues raised by smart grids.

52. For these reasons, the EDPS recommends that the Template should - at a minimum - require that the data protection impact assessment should assess certain key methods that may be used to minimize the amount of data processed. If a controller decides not to use these methods, its decision should be clearly justified in the impact assessment report. The EDPS also urges the Commission to outline these methods in the Template. These methods may include, among others, the following:

PETS to eliminate the need to export personal data from the household

- Innovative PETs exist, in different phases of research and development, which may make it possible to achieve the basic objectives of the smart metering system (billing, energy-efficient maintenance of the grid (forecasting and settlement), and maintenance of security (including prevention of fraud)), in such a way that it could be altogether avoided - for such basic purposes at least - that fine-grain meter-readings would need to leave the smart meter or the household where the smart meter is installed.³² The EDPS suggests that the Template recommend evaluating this option taking into account the state of the art, as well as cost of implementation.

Other methods to consider

- *Frequency of meter readings:* The intrusion to privacy greatly increases as meter readings become more frequent. The EDPS would welcome more guidance on this issue. In principle, in the absence of freely given, specific, explicit, informed consumer consent for a specific time-of-use tariff plan or for the provision of a specific value-added service that requires more frequent readings, individual readings should not be done and transferred more frequently than on a monthly basis.³³ The EDPS further recommends that even where time-of-use tariffs are in place - in the absence of informed consent for a very specific value-added service requiring more frequent readings - readings should not be done more frequently than once every half an hour or hour, and time-of-use tariffs should be developed accordingly, based on half-hourly, hourly, or less frequent billing periods. Any exceptions should be clearly justified by a compelling public purpose, and preferably clearly identified in legislation or regulation. For example, network operators might be given access to more frequent readings of individual

³² Such PETs may include software solutions that may be installed in the smart meters and which are capable of providing certified ('digitally signed') computations to network operators, energy suppliers or other parties concerned with regard to items such as the amount of the final bill payable, or aggregate data to help forecast energy needs and maintain the grid - without the need for fine-grain meter readings to leave the household and being shared with network operators, energy suppliers, or other third parties. In such a case, consumers would still be able to access their fine-grain data themselves (e.g. via the smart meter itself, or via devices such as smart phones or computers connected to the smart meter), and would be able to provide such data to third parties in a secure way, should they so decide, to obtain additional value-added services.

³³ See, e.g. Smart Metering Implementation Programme, Data Access and Privacy, Consultation document, referred to in footnote 24.

households for a specific purpose if they clearly demonstrate that collection of aggregate data at higher levels on the network is not sufficient for such a specific purpose. This might be the case, for example, if collection of data from an individual household is strictly necessary to manage the safe integration of the renewable energy source (e.g. solar panels) provided by the household to the network.

- *Sampling*: Use of sampling (i.e. collecting data of only a representative percentage of all households) could help eliminate collection and processing of data from all households for certain purposes (such as forecasting).³⁴
- *Aggregation combined with deletion*: For certain purposes, including forecasting, it should be sufficient to retain the fine-grain meter-readings until the aggregation has been computed. In such cases data may be deleted as soon as this is accomplished. (Data may be retained longer if also needed for other purposes such as billing and fraud detection).
- *Collection of aggregated data in the first place* (instead of collecting individual data, and subsequently aggregating such data): For certain purposes (including some purposes related to forecasting, network maintenance, and fraud detection), it should be sufficient for the operator of the electricity or natural gas distribution network to collect data from meters that are not measuring consumption of individual households, but rather, from meters that are placed at locations within the distribution network where they are measuring aggregate consumption of a number of households (e.g. a large apartment block, a street or a district). In these cases, for these purposes, collection of fine-grain data of individual households can be avoided altogether.

4.4. Clarification of roles and responsibilities of the different actors from a data protection point of view

53. Para 21 of the Recommendation requests Member States to determine the roles of the actors. The EDPS recommends that at least the Template itself should be more specific and should clarify which actors will be responsible in different situations (e.g. entities responsible for processing billing data, data necessary for forecasting energy needs, detect fraud, etc.). Additionally it should summarize which are the responsibilities as data controllers or as data processors that emanate from their roles.

54. In this respect, it would also be helpful if the Template provided definitions of the actors and used these terms consistently. This has not been done in the Recommendation itself. For example, in para 7 of the Recommendation, reference is made to 'network operators' and 'operators of smart metering systems'. Para 42(c), in turn, refers to 'the operator' and to 'the metering operators'. Recital 15 mentions 'the operator and stakeholders', while recital 18 refers to 'regulators, the metering industry, network operators and suppliers'. These terms, however, are not defined or further explained in the Recommendation.

4.5. Retention periods

55. As this has not been done in the Recommendation itself, the EDPS would now urge the Commission to also use the Template to bring more consistency with regard to

³⁴ Sampling - for some purposes - may be done on an opt-in basis; an alternative, which may be necessary for certain other purposes, is to collect data from each individual household, but not continuously, only intermittently, and for brief periods each time. The latter option is more intrusive than a purely opt-in solution, but often more reliable and may be necessary for certain purposes.

retention periods, by specifying, at least illustratively, the purposes for which it would be lawful to retain consumption data, a time limit for which retention would be proportionate for these purposes, and clarification of whether the purposes, in each case, would require retention of personal data or fully anonymized and aggregated data. In particular, the EDPS recommends that:

- these specifications be carried out at least for the basic purposes mentioned in Sections 4.1 and 4.2 above including billing, energy-efficient maintenance of the grid (forecasting and settlement) and maintenance of security (including prevention of fraud);³⁵
- the Template should clearly state that in principle, storage of fine-grain consumption data of individual households may be permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued (similar to what is foreseen in Article 6 of the e-Privacy Directive) and only to the level of granularity required for billing purposes;
- the Template should specifically require the establishment of sufficiently short retention periods. In the view of the EDPS, these retention periods should not, unless otherwise justified, exceed a period of a few months.³⁶ This should not, of course, prevent the retention of data for longer periods of time based on a specific, explicit consent of the customers concerned for specific purposes (for example, to obtain targeted energy advice).

4.6. Rights of the data subjects: access to meter readings, profiles, and right of correction

56. The EDPS would have welcomed more specific guidance in the Recommendation on how the rights of data subjects could be exercised in practice. A solution should be found to ensure that the data collected by the smart meters is made available to the consumers in a user-friendly way.

57. It would be preferable to provide a solution whereby the consumers did not depend on selected third parties (such as the operator of the smart metering system) to access their data but this could be done via a display on the smart meter itself and/or via an open inter-face on the smart-meter itself that the consumer would then be able to connect to the device of his/her choice (e.g. smart phone, laptop). Alternatively, if indirect, on-line access is foreseen, via the wide-area-network (WAN) of the operator of the smart metering system, it should be ensured that the data stored by such parties would only be accessible by the consumers themselves via secure on-line applications.

58. The EDPS would have preferred if these considerations (e.g. need for open interfaces) had also been more clearly reflected in the Recommendation with regard to the functional requirements of meters described in para 42. However, they should now be more explicitly required at least in the Template.

59. A further EDPS recommendation relates to tracking customer behaviour and data mining. In Section 4.2 above, the EDPS recommended informed consent for tracking

³⁵ For value-added services, the EDPS suggests that a recommendation be included for the actual length of the retention period to be established during the data protection impact assessment.

³⁶ When establishing retention periods, it should be considered that the rollout of smart metering systems will enable much more frequent readings, and consequently, much easier, and much faster billing, settlement, and forecasting practices. For these reasons, and unless specific justifications are provided to the contrary, it is reasonable to assume that it is possible to reduce longer regulatory periods foreseen for data retention, which were based on the assumption that meters are read only infrequently (for example, annually).

customer behaviour and profiling of individuals. In order for the consent to be valid, it must be genuinely informed. To achieve this, the EDPS recommends that customers should be given access to their 'profiles', as well as to the logic of the decision-making (algorithm) that lead to the development of the profile. They should also be able to correct or update their profiles. For example, if a market research company profiles one of its customers as a 'large high-income family, with young baby as well as teenage children, stay-at-home mother, always-on internet connection, frequent game-players and users of DIY equipment and gardening tools', this should be disclosed to the customer. The source of such information (e.g. tracking washing machine, bath fan, kitchen appliance use and other indicators to predict family size and type) should also be disclosed. Specific disclosures should also always be made if any sensitive data (e.g. health-related data) are collected.

60. Finally, the EDPS recommends that clear information should be provided to data subjects about the existence of any remote on/off switch functionality. This information should, among others, clearly describe the conditions under which energy can be switched off remotely. Information about adequate safeguards, such as access to the data and the logic underlying the decision of remote switch-off should be also specifically provided to the data subject to ensure that it can challenge any remote switch-off in a timely, efficient, and user-friendly way.

4.7. Data breach notifications

61. Para 28 of the Recommendation requires Member States to ensure 'in accordance with [the e-Privacy Directive]', that controllers notify 'the supervisory authority and the data subject' if 'the breach is likely to have an adverse effect on protection of his or her personal data'. The EDPS welcomes this recommendation. However, considering that the e-Privacy Directive is only applicable to providers of publicly available electronic communications services, and thus, it is unlikely to cover all situations when smart metering information containing valuable personal data can be compromised, the EDPS would recommend that all controllers processing smart metering data be made subject to the same requirement. In particular, as explained in para 40 above, the EDPS recommends including a provision in the Energy Efficiency Directive, requiring a mandatory data breach notification for all controllers processing granular smart metering data.

5. SPECIFIC RECOMMENDATIONS REGARDING THE DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

62. The EDPS, in this Section 5, briefly outlines his main expectations and recommendations regarding the Template currently under preparation. These recommendations complement, and should be read in conjunction with the recommendations provided in Section 4. The items discussed in Section 4 should have been preferably included in the Recommendation or in a binding legislative instrument. However, it may still be useful to include them – to the extent this is feasible, and with the necessary changes that the nature of a Template requires – in the Template.

The Template must offer specific and practical guidance: collection of best practice and 'best available techniques'³⁷

³⁷ For a definition of 'best available techniques', see EDPS website, glossary, at <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/72> .

63. To maximize the benefits that the Template may bring, the EDPS recommends that the Template provide stakeholders in Member States with specific and practical guidance on how to implement data protection principles to the deployment of smart metering and smart grid technology in practice. The Template must be pragmatic, flexible, but must also offer specific, principled, and consistent guidance on data protection issues to help ensure a high-level of data protection and a level-playing field across Europe. It should be possible to provide non-prescriptive and technology-neutral advice while at the same time avoiding that the Template remains at a too general level.
64. To achieve this, in particular, it would be useful if the Template also described, at least as illustrative examples, so-called 'best available techniques', as well as expected future techniques, that are recommended to be used to address data protection risks and concerns in specific situations.³⁸ Periodic updates of the Template (e.g. updates on 'best available techniques') could also be considered and would be welcome by the EDPS.
65. Preparation of the Template with specific and pragmatic recommendations, best practice, and best available techniques in mind is especially important considering that
- There is no specific legislation in place on the data protection aspects of smart metering and smart grid technology at the European level.
 - There is no binding legal requirement in current EU data protection legislation for the preparation of a data protection impact assessment, or further guidance on how such data protection impact assessment should be carried out. At national level guidance on impact assessments is also available only in some Member States. See, for example, the 'Privacy Impact Assessment Handbook' issued by the Information Commission's Office in the United Kingdom.³⁹
 - Finally, the fact that the Recommendation itself only provides high-level and general guidance on data protection issues also warrants more specificity in the Template itself.

Need for clear rules on methodology and process: who should prepare a data protection impact assessment and how to do it

66. The EDPS emphasizes that it would be crucial, as part of the Template, for the Commission to also outline how the impact assessment should be carried out and for the Template itself to follow a sound methodology. In this regard, the EDPS takes note of the intention of the Commission to use the 'Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications'⁴⁰ as a starting point of the development of the Template. This is not the place for the EDPS to provide an overview of best practice regarding data protection impact assessments, or a review of the achievements and of the shortcomings of the RFID impact assessment framework.
67. With this in mind, the following is a simple short-list of some key improvements that, in the view of the EDPS, are essential to ensure the effectiveness of the Template.
- *Mapping risks to safeguards.* The cornerstone of any genuine risk management process is to map risks to controls. In other words, it is crucial for the Template to clearly specify that the impact assessment must clearly match each risk with an

³⁸ For example, see Section 4.3, which lists some available techniques that may be used to minimize the amount of personal data collected.

³⁹ Available at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

⁴⁰ See footnote 9 above.

- adequate control. The Template must also be structured in a way to ensure this direct relationship between risks and controls.
- *Clear language and comprehensive descriptions.* The data protection impact assessment is a key tool that guides the controller to design data protection into its practices, technology and processes. In addition, it is also a tool for the controller to demonstrate compliance to data protection authorities and other stakeholders. To achieve this, the impact assessment, and the Template itself also, must use clear language, appropriate definitions and comprehensive descriptions.
 - *Who should prepare a data protection impact assessment?* The Template should also provide guidance to industry participants on who should prepare a data protection impact assessment. It should be ensured that all controllers⁴¹ responsible for the processing of personal data (for example, network operators as well as energy suppliers, and operators of the smart metering system but also providers of value added services) each carry out an impact assessment relating to their data processing activities.
 - Impact assessments can be prepared individually by each party (e.g. individually by each energy supplier and each network operator). However, considering the complexity of the data flows and the multiplicity of controllers and processors⁴², coordination of activities and exchange of best practice may be particularly important. When appropriate, it may even be useful, and may help development of best practice and avoid duplication of efforts if several parties prepare the impact assessment jointly. That said, clear allocation of liabilities is equally crucial, and joint efforts should not lead to lack of ultimate responsibility towards the data subjects.
 - As regards devices (such as smart meters and in-home displays), to ensure a data protection by design approach, and in particular, that data protection will be taken into account in the design of the functionalities of the devices, the EDPS recommends that a data protection impact assessment also be carried out for each device.
 - *Individual accountability.* The Template should ensure individual accountability, at sufficiently high-level within the organization.

6. CONCLUSIONS

68. The Europe-wide rollout of smart metering systems may bring significant benefits, but also entails considerable risks to the protection of personal data. It enables massive collection of personal data from European households and may lead to tracking what members of a household do within the privacy of their own homes. In light of these risks, the EDPS welcomes the Commission's efforts made in the Recommendation to provide guidance to Member States on the measures that should be taken in order to ensure that smart metering and smart grid systems are designed and operated subject to adequate data protection safeguards.
69. The EDPS appreciates the efforts of the Commission to make use of newly proposed concepts such as data protection by design and practical tools such as data protection impact assessments and security breach notifications. The EDPS, in particular, supports the Commission's plan to prepare a Template for data protection impact assessment and submit it to the WP29 for advice.

⁴¹ See Article 2(d) of Directive 95/46/EC.

⁴² See Article 2(e) of Directive 95/46/EC.

70. The EDPS regrets that the Recommendation has not provided more specific and more practical guidance on data protection. However, he considers that some guidance can still be given in Template currently under preparation. Therefore, the Opinion provides recommendations on the Template and emphasizes that the Template must offer specific and practical guidance: a collection of best practice and 'best available techniques'. It is also crucial for the Template to follow a sound methodology and, among others, clearly match each risk with an adequate control.
71. In addition, the Opinion calls on the Commission to assess whether further legislative action is necessary at the EU level and provides recommendations for such possible legislative action. Some of these recommendations can already be implemented via an amendment to the Energy Efficiency Directive, which is currently before the Council and Parliament. These should include at least a mandatory requirement for controllers to conduct a data protection impact assessment and an obligation to notify personal data breaches (Section 4.7).
72. Further, the EDPS also recommends:
- more guidance on the legal basis of the processing and the choice available to data subjects: in particular, a clear distinction between objectives for which energy usage data can be processed without customer consent, and those for which customer consent is required (Section 4.2);
 - mandatory application of 'PETS' and other 'best available techniques' for data minimization (Section 4.3);
 - clarification of roles and responsibilities of the different actors from a data protection point of view (Section 4.4);
 - more guidance on retention periods; in principle, storage of fine-grain consumption data of individual households should be permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued and only to the level of granularity required for billing purposes (without prejudice to the consumer's right for longer retention based on consent, for example, to obtain targeted energy advice) (Section 4.5);
 - direct access to consumers to their energy usage data; and effective methods to inform data subjects about the processing of their data; this should include, in case of data mining, disclosure of individual profiles and the logic of any algorithms used for data mining; comprehensive information regarding the existence of any remote on/off functionality should also be provided (Section 4.6).

Done in Brussels, 8 June 2012

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor