ARTICLE 29 DATA PROTECTION WORKING PARTY

00678/13/EN
WP205

Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force

Adopted on 22 April 2013

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

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

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

1 Context

1.1 Introduction

Background

On 9 March 2012, the European Commission issued a Recommendation on the preparation for the roll out of smart metering systems (the 'Commission Recommendation') in order to provide guidance to Member States for the rollout of smart metering systems in the electricity and the gas markets. The Commission Recommendation aims to provide guidance on data protection and security considerations, on a methodology for the economic assessment of the long-term costs and benefits for the roll-out of smart metering systems[1] and on common minimum functional requirements for smart metering systems for electricity.

With regard to data protection and security for the smart metering systems and the smart grid, the Commission Recommendation provides guidance to Member States on data protection by design and by default and the application of some of the data protection principles laid down in Directive 95/46/EC[2]. The Commission Recommendation further provides that Member States should adopt and apply a template for a data protection impact assessment ('DPIA Template'), which should be developed by the Commission and submitted to the Working Party on the protection of individuals with regard to the processing of personal data (WP29) for its opinion within 12 months of publication of the Commission Recommendation. Member States should then ensure that network operators and operators of smart metering systems take the appropriate technical and organisational measures to ensure protection of

1 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 (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). Directive 2012/27/EU on energy efficiency (OJ L 315, 14.11.2012, p. 1) includes additional provisions on smart metering. For the electricity market, Directive 2009/72/EC provides that when the roll out is assessed positively, at least 80% of consumers shall be equipped by 2020. No precise timetable is set forth for the gas market.

2 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 data, OJ L 281, 23.11.1995, p. 31–50

personal data in accordance with the DPIA Template, taking account of the opinion of the WP29 on the template[3].

The Commission Recommendation further provides that the DPIA Template should '*describe the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to assist in demonstrating compliance with Directive 95/46/EC, taking into account the rights and legitimate interests of data subjects and persons concerned*'.

Preparation

In February 2012, the Commission renewed the mandate of Expert Group 2 ('EG2') of its Smart Grid Task Force ('SGTF'), to provide a Smart Grid DPIA Template. EG2, which is composed mainly of industry representatives, held four workshops during 2012. The CNIL[4], the EDPS[5] and the ICO[6] attended these workshops as observers on behalf of the WP29.

On 26 October 2012, the WP29 sent a letter to the Directorate General for Energy of the European Commission ('DG ENER') in order to draw the attention of the Commission to several aspects of the draft DPIA Template that needed, in the opinion of the WP29, significant improvements. Among others, the letter recommended that the DPIA Template should

(i) clearly identify actors and their responsibilities,
(ii) focus on data protection and privacy risks to the individuals concerned,
(iii) better guide the actors to match each risk with adequate controls, and
(iv) offer more specific and practical guidance on how to address data protection and privacy risks in the smart grid context.

These comments were made without prejudice to the final assessment of the DPIA Template by the WP29.

DPIA Template

On 8 January 2013, the Commission submitted to the WP29 the final version of the DPIA Template prepared by EG2 stakeholders. In the letter accompanying the DPIA Template, the Commission noted that subject to WP29 comments and their appropriate reconciliation it may consider the adoption of the DPIA Template prepared by the EG2 stakeholders in the form of a Commission Recommendation[7].

---

[3] The EG2 took the experience gained from the development and revision, following comments and opinions from the Article 29 Working Party ('WP29'), of the 'Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' as a starting point.

[4] La Commission Nationale de l'Informatique et des Libertés, French national supervisory authority for the protection of personal data

[5] European Data Protection Supervisor, supervisory authority for the protection of personal data by EU Institutions and Bodies

[6] Information Commissioner's Office, national supervisory authority for the protection of personal data of the United Kingdom

[7] On 17 of January 2013 the DPIA Template was also submitted to the Council of European Energy Regulators (CEER). The president of CEER responded on 5 of March welcoming the work undertaken by EG2 and the resulting draft DPIA template. The letter reiterated the importance of

This Opinion provides comments on the proposed DPIA Template.

Structure of this Opinion

Section 1.2 highlights the importance of privacy and data protection for the successful implementation of the smart grid. Section 1.3 describes the objectives of the DPIA process. Section 2 contains the WP29's assessment of the DPIA Template. Section 3 draws the final conclusions. Annex I complements Section 2 by setting forth more detailed comments and suggestions.

1.2 Smart grids and data protection

The WP29 recalls its previous Opinion WP183 on smart metering[8], as well as the Opinion of the European Data Protection Supervisor ('EDPS') of 8 June 2012 on the Commission Recommendation[9].

Both opinions highlight the importance of data protection in the smart grid and smart metering context and provide guidance and recommendations on how to protect the rights to the protection of personal data in connection with the deployment of smart metering and smart grids in Europe. This Section will therefore only briefly describe the context and key data protection concerns.

Smart metering systems and smart grids aim at enabling intelligent and rationalised production, distribution and use of energy.

A key feature of smart gas and electricity 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. With smart meters it will be possible to read and record energy consumption very frequently, for example, every fifteen minutes.

Smart metering systems are important building blocks for the smart grid, which is an intelligent bi-directional electricity network that combines information from users of that grid in order, *inter alia* to plan the supply of electricity more effectively and economically.

The Europe-wide rollout of 'smart metering systems' enables massive collection of personal information from European households, thus far unprecedented in the level of detail and comprehensive coverage: smart metering may enable tracking what members of a household do within the privacy of their own homes and thus building detailed profiles of all individuals based on their domestic activities.

---

security, data protection and the need for the customers to be in control of their data; referred to previous CEER advice published in 2011; and called for rapid action in finalising the DPIA Template.

8 Opinion 12/2011 of the Article 29 Data Protection Working Party on smart metering, adopted on 4 April 2011 (WP183).

9 The EDPS Opinion is available on the EDPS website at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

From the detailed energy consumption data collected via the smart meters, a lot of information can be inferred regarding the consumers' use of specific goods or devices, daily routines, living arrangements, activities, lifestyles and behaviour[10].

The use of smart grids and smart metering systems, thus, creates new risks for data subjects with potential impact in different areas (e.g. price discrimination, profiling for behavioural advertisement, taxation, law enforcement access, household security) that were previously not present in the energy sector and were more typical and already present in other environments only (telecoms, e-commerce and Web 2.0).

Smart metering is also among the first widespread applications that foreshadow the future of 'the Internet of Things'. The risks posed by the collection and availability of detailed energy consumption data are likely to increase in the future considering the increasing availability of data from other sources, such as geo-location data, data available through tracking and profiling on the internet, video surveillance systems, and radio frequency identification (RFID) systems, with which smart metering data can be combined[11].

1.3 Objectives of the DPIA Template

With its Recommendation, the European Commission aims to encourage data controllers to carry out a DPIA with a view to achieve the following benefits:

- A DPIA should describe the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC..

- A DPIA should also help national Data Protection Authorities to assess the compliance of the processing and, in particular, the risks for the protection of personal data of the data subject and the related safeguards, when data controllers consult them prior to Data processing, as provided for by the Commission Recommendation[12]. DPIAs, thus, should also assist the data controller in demonstrating compliance with Directive 95/46/EC[13]

[10] To illustrate, with a 2 second reading interval, it has been demonstrated that it was even possible to identify what multimedia content was consumed in the household: http://www.its.fh-muenster.de/greveler/pubs/preprint_online.pdf.

[11] Recommendation CM/Rec(2010)13 of 23 November 2010 of the Council of Europe Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

[12] This recommendation is without prejudice to a legal obligation for prior checking in Member States, according to the characteristics f the processing operations.

[13] 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 data. OJ L 281, 23.11.1995, p. 31

Furthermore, DPIAs may help consumers, data controllers, data protection authorities, energy regulators, consumer protection organizations and other stakeholders, to gain more insight into the specific data protection aspects of smart metering and smart grid applications. Information from DPIAs may also help DPAs identify both best practices and possible high risk target areas for audits.

In Member States where prior notification/checking is required for smart metering and smart grid applications the DPIA may simplify the process for both the DPAs and data controllers. DPIAs, thus, should also assist the data controller in demonstrating compliance with Directive 95/46/EC.

Finally, it is to be highlighted that the proposed Data Protection Regulation[14] would increase the importance of the DPIA process, which is seen as a key tool to help ensure the accountability of data controllers.

1.4 Summary of the proposed DPIA Template

The EG2 explains that it took the experience gained from the development and revision, following comments and opinions from the Article 29 Working Party ('WP29'), of the 'Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications', as a starting point for its work.

The DPIA Template proposed by EG 2 first explains the objective, the scope, the benefits and the stakeholders of the process. It then develops an approach allowing to conduct a DPIA in eight steps and gives step by step guidance to the data controller on how to carry out the DPIA itself.

2 Analysis of the DPIA Template

The WP29 acknowledges the extensive work conducted by EG2 stakeholders, and welcomes its main objectives, highlighted in the introductory sections of the DPIA Template.

While - in general - the eight-step approach outlined in the proposed document is sound, the WP29 has identified several critical concerns about the methodology, as well as the content of the DPIA Template itself, which are detailed in the following sections.

2.1 Lack of clarity on the nature and objectives of the DPIA

As defined in Section 3(c) of the Commission Recommendation, a data protection impact assessment '*means a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*' to be carried out by the controller or the processor acting on the controller's behalf.

[14] On 25 January 2012, the Commission adopted a package for reforming the European data protection framework. The package includes (i) a 'Communication' (COM(2012)9 final), (ii) a 'Proposed Data Protection Regulation' (COM(2012)11 final), and (iii) a 'Proposed Data Protection Directive' (COM(2012)10 final).

The WP29 supports this definition and the objective of a DPIA should thus be to assess the impacts of the risks on the data subjects.

The WP29, however, regrets that the submitted DPIA Template does not directly address the actual impacts on the data subjects, such as, for example, financial loss resulting from inaccurate billing, price discrimination or criminal acts facilitated by unauthorised profiling. Even if the data protection and privacy targets listed in Annex I can be very useful to facilitate compliance, they are not sufficient in the context of a risk driven approach. Assessment of the potential impacts on data subjects is an indispensable element of such an approach.

Therefore, the WP29 considers that the DPIA Template in its current form cannot achieve its objective mandated by the Commission Recommendation. The DPIA does not provide a practical tool for assessing the impact on the individuals concerned.

If the risks and their impact on data subjects are not considered in their entirety, it is not possible to correctly identify and implement the necessary controls and safeguards.

2.2 Methodological flaws in the DPIA Template

In addition to, and sometimes linked to, the key shortcoming identified above, the WP29 believes that the DPIA Template suffers from a number of methodological flaws that jeopardise its application.

Firstly, the proposed DPIA Template often confuses risks and threats.[15]

Secondly, there is no matching between the risks to be mitigated and the list of possible controls in Annex II. Even if each risk scenario is specific and should be assessed in its peculiarity, it is often possible to identify certain categories of controls as being effective in mitigating certain risk categories. A typical example of this is given by the information security standard ISO/IEC 27002:2005 where controls are presented as best practices to mitigate risks in certain areas. Suggested mitigating measures, while not replacing the need for a risk driven process, can provide a reference for an effective and coherent approach. For example, the risk of consumers' energy consumption data being intercepted along an unprotected channel can generally be mitigated by encryption techniques. The specific risk assessment could then lead to the choice of certain encryption algorithms and key lengths or of alternative or complementary mitigating measures or even to risk acceptance or risk transfer (and thus no mitigating measures).

---

[15] See ISO/IEC 27005:2008 definition of risk in the field of information security as 'the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization'. Threats do not have a direct definition but an operational definition can be derived from ISO/IEC 27001:2005. Accordingly, threats refer to the ability to exploit vulnerabilities on the assets to be protected. This will then have an impact on these assets in terms of loss of security properties. Example of typical security related threats are listed in annex C of ISO/IEC 27005:2008.
See also CNIL methodology: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf and the ENISA threat landscape: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport).

In addition, the proposed DPIA Template also does not give enough detail and specific guidance on the concept of vulnerability, on how to calculate and prioritise risks, choose the appropriate controls and assess the residual risks that remain after the controls have been put in place. Although a reference is made to an external document, the WP29 would have welcomed more guidance and more explanation in the DPIA Template itself, in order to provide the reader with a stand-alone document. It is also not clear how to complete the proposed forms.

Finally, the DPIA Template does not provide sufficient advice on how to determine data protection roles and responsibilities of the different stakeholders. Only a reference is made to another EG2 document. The upcoming smart grid applications will be various, and offered by multiple stakeholders. Therefore it seems critical to provide the industry with guidelines allowing the identification of data controllers and data processors. For example, the DPIA Template could include in the third step a fourth section aiming at determining the different responsibilities of the various entities involved in the data processing.

Further details on these and additional shortcomings in methodology are provided in Annex 1.

2.3 The DPIA Template lacks sector-specific content: industry-specific risks and relevant controls to address those risks should be identified and matched

The DPIA Template lacks sector-specific content. Both the risks and the controls listed in the template are of generic nature and only occasionally contain industry-specific guidance - best practice that could be genuinely useful. In a nutshell: the risks and controls do not reflect industry experience on what the key concerns and best practices are.

The WP29 understands that the EG2 is currently working on a collection of ‘best available techniques’ ('BATs') that would enable an organisation conducting a DPIA to choose the adequate measures if necessary, therefore addressing some of the criticism raised in the previous Section. The WP29 insists on the importance of this document, which is complementary to the DPIA Template.

However, the BATs document cannot substitute for the identification of the most common industry-specific risks and possible controls matching those risks in the DPIA Template itself. This is all the more true as – unlike this DPIA Template – the BATs document will not be submitted to the WP29 for further evaluation and guidance and is not planned to be adopted by the Commission. Given the identified shortcomings of the DPIA Template, the Commission should consider integrating the BATs into it and submit the integrated document to the WP29 for an opinion.

In addition, the notion of a DPIA template is different from the notion of a DPIA framework. A framework should identify objectives, outline a methodology and define the scope of the assessment in terms of the boundaries of the system/process under analysis. A template should go further and provide an operational instrument to manage the risks of the specific system/process and its use cases, suggest possible

controls and best available techniques to mitigate those risks and provide specific guidance. This is particularly needed in cases where no specific expertise is at disposal (SMEs, for example, or as in the smart grid case, in an industry that has previously faced relatively few privacy and data protection issues).

The DPIA Template should aim at developing more sector-specific and easier to use guidance. In particular, it is necessary to better define potential impacts on the data subjects in the smart-grid context and to give more precise guidelines regarding the type of controls that can be implemented.

The Commission could have provided EG2 a generic privacy and data protection risk assessment methodology[16]. EG2 could have, in turn, applied such a methodology, and based on such methodology, could have made the DPIA Template more sector-specific. This approach would have allowed EG2 to focus on relevant issues such as smart grid specific risks and controls while relying on the reference framework for fundamental methodological aspects. The WP29 suggests that the EG2 and the Commission take this approach for the future development of this DPIA Template and for any other sector-specific DPIA templates.

3 Conclusion and recommendations

The WP29 recognises the progress made from earlier versions and the useful elements that the DPIA Template already contains. Nevertheless, it is of the opinion that the DPIA Template in its current form is not sufficiently mature and well-developed.

Therefore, the WP29 recommends the Commission to take the necessary steps to ensure that work on the DPIA Template continues and that the final deliverable will provide sufficiently specific, useful and clear practical guidance to data controllers.

To facilitate further work, the WP29 provides some more specific recommendations in Annex 1 to this Opinion. However, considering the methodological flaws of the document and its lack of specificity to the smart grid context, the WP29 is not in a position to provide further, more detailed and conclusive, input at this stage.

Given the identified shortcomings of the DPIA Template, the WP29 further recommends that the Commission should consider integrating the BATs into the DPIA Template and submit the integrated document to the WP29 for an opinion.[17]

Further, and more broadly, the WP29 recommends the Commission to consider taking stock of past and on-going work in the field of DPIAs[18] and to consider the opportunity of defining a generic DPIA methodology from which field specific efforts could benefit.

---

16 See, for example, CNIL methodology already cited above.

17 This does not exclude that the BATS document could be periodically updated in the future to reflect technological changes and state of the art.

18 See, for example, PIAF Project: http://www.piafproject.eu/Index.html as well as the existing methodologies referred to earlier.

Finally, with regard to the need for a mandatory impact assessment, the WP29 refers to the experience gained with the RFID PIAF and emphasises that available statistics in Member States shows that the take-up of impact assessments for RFID has been extremely low. Whereas these statistics may have several underlying reasons, one of the key contributing factors definitely appears to be the current lack of a mandatory requirement to carry out such an impact assessment.

Done at Brussels, on 22 April 2013

For the Working Party
The Chairman
Jacob KOHNSTAMM

Annex 1: Specific comments on the DPIA Template

This Annex complements Section 2 of the Opinion. Structure of comments follows the structure of the DPIA Template.

→ Scope of the DPIA

- The template does not provide a precise definition and description of the types of data processing that are subject to a DPIA. Further, the scope of the DPIA is not accurately defined in Section 1.2 of the DPIA Template. The Commission Recommendation clearly defines DPIAs as a 'systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes'. This definition includes the fundamental rights defined in Articles 7 and 8 of the European Union Charter of Fundamental Rights (the 'Charter'), respectively the right to privacy and the right to the protection of personal data. It should be taken into account that the template is related to the protection of personal data as defined in Directive 95/46/EC.[19]
- As highlighted in the general comments, the DPIA Template should focus on the impact on the data subject. Whereas meeting the privacy and data protection targets identified in Annex I, and compliance with data protection law must be achieved, compliance with data protection law is not a goal in itself and for its own sake. The ultimate objective of the DPIA process thus is to identify controls that minimize any negative impact on the rights and freedoms of the data subjects.
- The following examples may help illustrate the difference between an approach that is reduced to a mere compliance check and one that is based on the assessment of real life risks with corresponding real life impact on data subjects.
    - Crime-related risks: If the technical and organizational measures taken to ensure the security of energy consumption data are inadequate, the energy consumption data of an individual household may be unlawfully accessed. This may increase the risk of the consumer concerned falling victim to crime. For example, knowing the behavioural pattern that can be inferred from energy consumption data, in particular that a house is empty at a particular time, might lead to an increased risk of break-ins and theft.
    - Individuals may be wrongly billed if the energy consumption data are tampered with.[20]
    - Profiling, exclusion, discrimination, unsolicited marketing: increased availability of data on smart grid consumers may lead to increased profiling, which, in turn, may lead to price discrimination and exclusion (e.g. blacklisting, higher tariffs), unsolicited targeted

[19] Any reference to the concept of 'data privacy', or attempts to provide an *ad hoc* definition for 'privacy' in Section 1.2 or in the Glossary are unnecessary and could be misleading. The terminology of Directive 95/46 should be used wherever possible. Articles 7 and 8 of the Charter can be quoted and referred to for further guidance.

[20] Similar risks may also apply to owners of solar panels or micro-cogeneration plants with regard to their billing.

behavioural advertisement, as well as an overall imbalance in the economical situation of the consumer vis-à-vis the service providers/data controllers that can subsequently be misused.

- Risks of incompatible and unlawful use by law enforcement or other third parties, risk of increased government surveillance (which could be mitigated, for example, by minimising the personal data processed).

- The above and other examples of risks and possible impact on data subjects should be considered and included in the impact assessment.

→Stakeholders

- The DPIA Template does not consider the roles and functions of the different actors in the smart grid ecosystem and, accordingly, does not distinguish their responsibilities. However, smart grids can only achieve their objectives with an organized cooperation and an exchange of data between the different participating organizations. In order to produce a meaningful DPIA, participants will have to work together. The proposed DPIA Template does not give sufficient guidance on how to carry out a DPIA when several operators are involved and carry out related data processing activities.
- In Section 1.3.3. 'smart grid operator' is a very generic term and does not take into account the fact that different actors can perform different functions in the smart grid landscape, which strongly influences the boundaries and scope of the DPIA carried out[21]. These functions should be described with a specific accent on their role in the exchange of personal information necessary to run the smart grid business processes. A concise and up-to-date definition of the roles of the parties involved in the DPIA process should be included in the DPIA Template (see, for example, the EG2 report of 16 February 2011[22]).
- A reminder about the need to comply with applicable legislation should be added.
- The DPIA Template should also mention as stakeholders (i) recipients of the data and (ii) the Data Protection Officers (if any) of the organization.

→ Step 1

- The pre-assessment criteria need reconsideration. Accordingly, the questionnaire in Section 3.1 also needs reviewing. This is also necessary in order to ensure consistency with Section 2.1.
- The order of the criteria should be changed in order to follow the logical order in which they should be examined:
    1. Are personal data being processed?
    2. Is the organization the data controller?
    3. Are there any impacts on rights and freedoms due to the data processing?
    4. When will be the right time and what will be the motivation?

[21] See, for example, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGConceptualModel#Smart_Grid_Conceptual_Model_Doma.

[22] See http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

- Among the types of data that are listed in the DPIA Template as such that can be considered as personal data, some are clearly not personal data (demand forecast of building, campus and organization). In contrast, some data that can be personal data are not listed or wrongly listed (the inside temperature of a house can be personal data since it can show whether or not the house is occupied by an individual; the successive locations on which an electrical car has been charged is personal data, since it shows the location of the user, etc.). More guidance should be given in order to help the organization identify the personal data that will be processed.
- Further, also on Criterion 1, a DPIA should also be performed for existing systems that have not been built with 'Data Protection by Design' in mind, and for which no DPIA has been carried out previously. This should be highlighted in the text, for example, in an additional bullet point in the list of triggering elements already drafted under the heading 'Right timing', or in a separate paragraph following the bulleted list.

→ Step 2

- It is important to ensure, when the resources of the organisation allow it, that the team conducting the DPIA is independent from the team working on the smart grid application itself. This will contribute to fairness and objectivity of the DPIA: this requirement is not included in the document.

→ Step 3

- The description of the system lacks a clear description of the assets on which the processing of personal data rely (e.g. a database acting as a repository of the data collected in a certain area). This would be important since some of the threats will also target those assets. The different types of personal data processed must also be comprehensively identified, as well as the purposes and the way in which they are processed. Their proposed retention periods must also be indicated.

→ Step 4

- This step mostly relies on the list of threats listed in the questionnaires of the DPIA Template. There seems to be confusion between threats and risks (see Section 2.2 of this Opinion). Furthermore some of the items listed concern 'lack of measures' (e.g. insufficient logging mechanism, lack of unification in subject access requests mechanism) rather than threats.

→ Step 5

- The impact of the data protection threats is weighted in terms of impact on the privacy and data protection targets identified in Annex I, and not in terms of impact on the individuals (data subjects) concerned. Furthermore, the DPIA Template itself does not contain adequate guidance on the type of impact and on the methodology.

- The likelihood of materialisation of the risk is described as the combination of the level of vulnerability and the ease of exploitation of the vulnerability. However, since the assets supporting personal data have not been identified in step 3, there is no indication of what the vulnerability refers to.

→ Step 6

- It is also crucial for the DPIA Template to clearly match each risk with one or more adequate controls for risk mitigation (while making it clear that, where relevant and appropriately justified, some risks can also be transferred or accepted). This relationship should become a core element of the document. The current structure of the Template does not support such an integrated approach, as the WP29 already pointed out in its October 2012 letter.
- With regard to residual risks (Section 6), as the WP29 already mentioned in its October 2012 comments, the right to the protection of personal data is a fundamental right, and compliance with it is a clear and high-level legal requirement. This should be more clearly highlighted when referring to the possibility of accepting some degree of residual risks: it could be explained that irrespective of the outcome of any risk assessment, data protection and privacy targets must be met: for example, data subjects must be given appropriate notice in all cases and there must also be a lawful ground for the processing (e.g. a legal obligation or consent by the data subject). It is crucial to be very clear about the fact that data protection law must be complied with in all cases. The risk assessment can help identify how to best comply with data protection law. For example, what type of encryption to use in order to ensure the appropriate level of security for the data, what can be considered as a proportionate retention time, or how best to minimise the amount of data collected and further processed. However, the risk assessment should not be used to provide an excuse for not meeting legal requirements in cases where the risks are perceived to be comparatively lower. As a more general consideration relating to this issue, there is no advice on the way of determining the level of the residual risk that can be accepted.

Annex II List of possible controls

The controls listed in Annex II are not sufficiently specific so as to provide any useful guidance to the controllers. Most of them also do not address the specificities of the smart grid context and do not reflect industry experience on what the key concerns and best practices are.

To illustrate our expectations regarding the level of detail and practical examples we would expect from the Template, we would like to highlight some of the most important issues that in our view the Template should address thoroughly.

Legal basis and choice

The WP29 would like to see in the Template more guidance on what legal basis to choose for the processing and what choice should be made available to data subjects. In particular, there should be a clear guidance on what can be done without user consent, and what requires user consent. Particular attention should be given to the implementation of the remote switch-off and granular readings.[23]

In most cases, a freely given, specific, informed and explicit consent would 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[24], and (iv) preparation of aggregated data necessary for energy-efficient maintenance of the grid (forecasting and settlement).[25] Examples where consent would be required include tracking and profiling for targeted advertisement.

For consent to be valid, consumers need to understand what happens to their data. Importantly, in case of profiling, they should have the right to know their individual profiles and the logic of any algorithms used for data mining. Information on remote on/off functionality is equally important: customers need to know what events can trigger a switch-off.

Data minimization and privacy enhancing technologies

The DPIA Template should also encourage the companies concerned to ensure that only as much personal data is collected and processed as it is absolutely necessary. To achieve this, several methods can be considered and we recommend that at least the most common privacy enhancing technologies ('PETS') and other 'best available techniques' for data minimization would each be described briefly and in a technologically-neutral manner in the DPIA Template, and then be further detailed, in the accompanying BAT document to be produced by the EG2, to help promote data-protection friendly deployment of smart metering and smart-grid technologies.

---

[23] See, e.g. para 48 of the EDPS Opinion of 8 June 2012, referenced in footnote 3 above.

[24] Of course, data processing for purposes of detection of fraud must still comply with all other relevant data protection safeguards, including the requirement for proportionality, and the principle of data minimization.

[25] Where applicable, these purposes, for which no consent is required, usually coincide with the regulated duties of the data controllers.

In particular, innovative PETs exist, currently 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 security assurance (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. In addition, the following could be discussed:

- Frequency of meter readings: The intrusion to privacy largely increases as meter readings become more frequent. The WP29 would welcome further guidance, including some references[26] and examples on this issue in the DPIA Template.
- 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). Examples here also should be included in the DPIA Template.
- Aggregation combined with deletion: For certain purposes, including forecasting, it should be sufficient to retain the fine-grain meter-readings only until the aggregation has been computed. In such cases data may be permanently deleted as soon as this is accomplished. Again, examples should be provided.
- 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 gas distribution network to collect data from meters that do not measure consumption of individual households, but rather, from meters placed at locations within the distribution network where they can only measure 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. Again, real-life illustrative examples would be helpful in the DPIA Template to encourage compliance with data protection law and good practice.
- To help minimize not just the amount of data collected, but also the time period for which data will be retained, the DPIA Template should also provide more guidance on retention periods. In our view, in principle, storage of fine-grain consumption data of individual households collected for billing purposes should be permitted only up to the end of the period during which the bill may lawfully be challenged or payment pursued. (This is, of course, without prejudice to the consumer's right for longer retention based on consent, for example, to obtain targeted energy advice, and to other possible lawful purposes.)

[26] See EG2.P.1 in "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection" (http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf)

Glossary

The WP29 recommends that the Glossary be carefully reviewed to ensure that terminology is in line with the current language of Directive 95/46/EC and also compatible with the proposed new data protection framework.