ARTICLE 29 DATA PROTECTION WORKING PARTY

2064/13/EN
WP209

Opinion 07/2013 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

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 Recommendation 2012/148/EU 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 report produced from the application of the template, taking account of the opinion of the WP29 on the template[3].

The Commission Recommendation further provides that the 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 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, has held several workshops since where representatives of the WP29 attended as observers.

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.

First issue of the DPIA Template

On 8 January 2013, the Commission submitted to the WP29 the first 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[4].

The WP29 issued its Opinion 04/2013 on 22 April 2013. The Opinion on the one hand acknowledged the extensive work conducted by EG2 stakeholders and welcomed the objectives set. On the other hand several critical concerns were identified, which can be summarised as follows:

i. lack of clarity on the nature and objectives of the DPIA;

ii. methodological flaws in the DPIA Template;

iii. lack of sector-specific content: industry-specific risks and relevant controls to address those risks to be identified and matched.

The WP29 concluded that the DPIA Template was not sufficiently mature and well-developed and invited the Commission to make so that the work on the DPIA

[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] 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 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.

Template continues to eventually ensure a sufficiently specific, useful and clear practical guidance to data controllers.

The WP29 also invited the Commission to consider integrating the Best Available Techniques (BATs as defined by point 3.f of the Recommendation) into the DPIA Template and submit the integrated document to the WP29 for an opinion. It also recommended that Commission consider taking stock of past and on-going work in the field of DPIAs and the opportunity of defining a generic DPIA methodology from which field specific efforts could benefit.

Second issue of the DPIA Template

The Commission replied to the WP29's Opinion on 27 May 2013. The letter reported a request by the Commission to the EG2 for a revised Template and acknowledged the WP29's availability to some support, while keeping its specific role, for the works of the EG2. Furthermore the Commission has preferred not to integrate the BATs into the Template reportedly because of their scope limited to the common minimum functional requirements for smart metering and their evolutive nature[5]. On the proposal to define a generic DPIA methodology from which field specific initiatives could benefit, the letter called on another competent department of the Commission, from which no answer has been received so far.

The EG2 created an editorial team for the second draft of the Template, which met on 4 June and 3 July 2013. Some representatives of the WP29 participated in the first meeting as observers and replied to inquiries from the EG2 representatives on the various issues raised in the Template.

On 20 August 2013, the Commission submitted to the WP29 the final version of the revised DPIA Template prepared by EG2 members.

Structure of this Opinion

Section 1 reports the events leading to the revised DPIA Template and refers to sections of Opinion 04/2013 as to the issue of data protection in smart grids and the objectives of the DPIA in that context.

Section 2 contains the WP29's assessment of the revised DPIA Template.

Section 3 draws the final conclusions.

[5] "*I consider this that would not be as beneficial as you intend for the following reasons: (i) In line with the Commission Recommendation 2012/148/EU, the BATs focus only on the common minimum functional requirements for smart metering, whereas the DPIA template's scope of application strives to go beyond the last mile and include the whole smart grid spectrum; and (ii)Should the BATs be enshrine in the DPIA template, their evolutive and illustrative nature would ipso facto condemnthe template to be ephemeral and possibly subject to impractically frequent revisions*."
(letter ener.b.3 VL/cv(2013)1506536 to Mr. Kohnstamm, 27 May 2013)

1.2 Data protection in smart grids and the objectives of the DPIA in that context

Sections 1.2 and 1.3 of Opinion 04/2013 already addressed the issues of data protection in smart grids and the objectives of the DPIA in that context. The WP29 does not have any new elements to add on these issues.

2 Analysis of the DPIA template

The WP29 welcomes the work conducted by EG2 members in an effort to address WP29's comments and their willingness to take the advice of the WP29 into account as a valuable support.

This analysis mainly follows up the comments made in Opinion 04/2013. It also includes improvements and optimizations that should be considered to finalize the Template. The sections below take account of both aspects.

In order to have a comprehensive and clear understanding, the analysis needs to be read in the light of the content and the terminology of Opinion 04/2013.

2.1 The DPIA Template and the EC Rec. 2012/148

The WP29 has taken the opportunity to closely review this second issue of the smart grid DPIA Template in the light of the Commission Recommendation, which provides for its purpose, scope and applicability.

2.1.1 On the discretional nature of performing a smart grid DPIA

The existence of a Commission Recommendation, while on the one hand not imposing a legally binding obligation, on the other hand sets forth that certain measures are strongly recommended. Rec. 2012/148/EU provides that the processing operations of personal data in smart meters/smart grids need a "*systematic process for evaluating the potential impact of risks... the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". The WP29 wants to reaffirm that the need for such a process, already established in WP29 Opinion 12/2011 on smart metering in the context of a "privacy by design" approach, is largely justified by the complexity of smart grids technical and management infrastructure, by its potential scale of application and evolution, and by the specific risks for the individual's fundamental rights and freedoms, including, among others, life (e.g. switch off of energy supply where certain powered machines support vital functions).

Furthermore, the WP29 has welcomed the fact that the Commission has proposed a General Data Protection Regulation that would make data protection impact assessments mandatory under certain conditions. It should be clear for the stakeholders of the Smart Grid DPIA template, i.e. data controllers and processors, that the use of the template should be seen as a means to comply with a legal obligation in the future. Given the huge investments and the long planning horizon for utility networks, it should be understood as being in the genuine own interest of the stakeholders to already collect experience with the DPIA approach and to apply it already from the start in designing their systems, so that they would not face

compliance issues when the currently pending legislation enter into force. Where the language used in the present template, especially in section 2.1, could be read as leaving considerable margin for a widely discretionary approach by the enterprise, the Commission should ensure that clarification is provided that such margins should be interpreted in a strict manner, ensuring that an actual DPIA is performed in the most comprehensive way possible, e.g. by explaining this approach in a Commission Recommendation that might accompany and support the template. The WP29 interprets the role of the pre-assessment as functional to take into account all possible situations prospective controllers and processors might face, based on the information processed, the scope of the (sub)system under analysis, the status of the project etc., and not as a step in the methodology weakening the Commission Recommendation objectives.

2.1.2 The DPIA and the Data Protection authorities

Point 8 of the Commission Recommendation provides that Member States should ensure that the entity processing personal data consult their DPAs on the data protection impact assessment, prior to processing. The WP29 notices that the template is not fully reflecting this approach in many parts. Some quotations: "in case of doubt" (section 2.1.4), or just consult the DPO (not the DPA) "when available" (section 2.6.2), or to be submitted to the DPA "if requested" once the final report is adopted (section 2.7). While it would be preferable if the template would make consistently clear that, unless national DP law and/or DPA's national policy provide explicit exception, national DPAs should be consulted prior to processing as recommended by the Commission Recommendation, the Commission should ensure in an appropriate manner that stakeholders obtain clarity that the DPIA template adopted under its Recommendation cannot change the principles adopted by the Recommendation as such. The referenced passages can only be understood as advising additional possibilities to obtain advice, which are complementary to the consultation of the DPAs, as recommended by the Commission.

2.2 Clarity on the nature and objectives of the DPIA

2.2.1 Considering the final impact on individuals' rights and freedoms

The WP29 welcomes that the risk assessment step of the methodology outlined in the Template (section 2.5) aims to consider the actual impacts on data subjects' fundamental rights and freedoms and civil liberties (such as, for example, financial loss or price discrimination or criminal acts facilitated by unauthorised profiling) as effects of the "feared events" due to unfair and unlawful processing of personal data, and not any longer the impact on the privacy targets as such.

Nevertheless, some confusion seems still to exist in the text explaining the risk assessment methodology (see relevant section in this Opinion) and particularly in section 2.5.1.1 of the Template, describing how to assess the impact of feared events. In particular the sentence trying to identify the elements to assess "*the impact and severity of a certain identified threat*" does not bring any clarity. It mentions the privacy targets as elements of this assessment (see section 2.2.2 in this Opinion) without elaborating on and explaining how they fit in, singles out "*crime related*

risks" without evident reason and lists apart elements such as "*freedom to move, loss of independence, loss of equality*" calling them "*other privacy principles*[6].

The WP29 would like to underline that the DPIA always and consistently assesses the impact on the "*rights and freedoms of data subject"*, as reminded in section 2.1 of Opinion 04/2013, and correctly stated in several parts of the template. Where the template uses different terminology, e.g. referring only to the right to privacy, this must be read as referring to the more comprehensive concept. This should be addressed in future revisions of the template.

Moreover, if it is true that the same feared event might lead to many impacts on data subjects, it could be useful, for more awareness and with a view to impact sizing, to list the most relevant impacts on data subjects relating to the feared events in the examples given at section 3.4.1. This link between the feared event and the impact on the individual's fundamental rights and freedoms characterizes this effort in the context of the protection of individuals as regards the processing of personal data as opposed, for example, to a mere assessment of information security risks.

2.2.2 The privacy targets handling

The way to handle the privacy targets is one of the most important issues in a PIA. Indeed, its goal is to ensure that privacy targets have been correctly considered.

Currently, privacy targets are:

- mentioned in "2.5.1.1 Impact of feared events" as elements to be considered when assessing the impact and severity of a certain identified threat;
- mentioned in "2.6.3. Residual risks and risk acceptance" as goals to be reached;
- listed and described in "Annex 1. Privacy and data protection targets".

Directive 95/46/EC[7] defines in most of its provisions specific conditions for the processing of personal data and a set of obligations that data controllers and processors have to comply with. The Directive does not provide for a margin of discretion or for acceptable levels on non-compliance with these provisions. While ensuring the security of processing is one of these obligations, for its implementation the Directive provides in its article 17 for a risk management approach by stating that "Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected". In the context of an impact assessment template, it is important to be aware that risk management strategies as

[6] A suggestion could be of augmenting the last sentence of the first paragraph of "2.5.1.1. Impact of feared events" with other elements; phrasing it this way: "This potential impact is defined by the consequences each feared event could have on data subjects's privacy and other fundamental rights and freedoms, including e.g. crime related risks such as identity theft and fraud, or freedom to move, independence, equal treatment, social relationships, financial interests, etc. due to e.g. profiling, unsolicited marketing, discrimination or individual decisions on wrong information…"

[7] 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.

those developed in the security domain may be applied for data protection, but only with respect to security issues, and that for the majority of obligations full compliance is required. The template uses the term 'privacy targets' to designate the compliance obligations and it clarifies in its section 2.6.3 that the concepts of residual risks and risk acceptance do not apply to these privacy targets which "have to be reached" (p. 33).

WP29 welcomes that this distiction between risk management and compliance is recognized in the template, but would have welcomed a clearer and more visible presentation.

Accordingly, there should always be two distinct and complementary actions to address the findings of a DPIA. The first action is related to risks on personal data. They should be subject to risk management (assessed, treated etc.). The second action relates to the compliance with the privacy targets as such, as legal obligations. This should be considered as compliance issues (measures implemented or planned to reach the privacy targets, justification if it is not done, legal risks of not doing it, planned controls to check whether and how it is done or not...).

As regards the risk analysis, it should be highlighted that the feared events described in "2.4.1. Introduction" should be systematically assessed. Their potential impacts on data subjects should be identified, the estimation of prejudicial effects should be based on those potential impacts. Nevertheless, the Commission may want to verify what distinguishes the last feared event (diverting of personal data … to people who have no need) from the third one (illegitimate access to personal data … by unauthorised persons).

The WP29 wants to suggest some tools to complement the methodology proposed in the template, in order to facilitate its applicability. It invites the Commission to make these suggestions known to potential users of the template, e.g. by making the present opinion available with the template or referring to it in any accompanying instrument. The complementary tools are described in the Annex of this opinion.

2.3 The methodology used in the DPIA Template

Overall the methodology outlined in the Template has been clarified and is more actionable. Nevertheless, many unclear and confusing elements remain, including in the list of generic threats provided in section 3.4.1, in the Template forms and questionnaire provided.

Some of these elements have been dealt with in section 2.1 while addressing the issue of clarity on the nature and objectives of the DPIA. The others will be addressed here.

2.3.1 The risk assessment (management) methodology

Most of the elements of the risk management methodology are reportedly mainly based on ISO 31 000, EBIOS methodology and the synthesis produced by the CNIL[8].

[8] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

Assets identification

A definition of primary and supporting assets exists as targets of the overall risk assessment.

Threats and vulnerabilities identification and assessment

The distinction between threats and risks is now defined. There is more guidance on the concept of vulnerability.

Nevertheless, the WP29 is concerned that the presentation of missed privacy targets as generic threats listed in section 3.4.1, in particular in section 3.4.1.4, could lead to the misunderstanding that the template would "define a missed privacy target as a threat" in order to fit the assessment of the privacy targets in the context of the risk assessment methodology. This issue has already been discussed in section 2.2.2 of this Opinion.

The WP29 acknowledges, though, that relevant examples and the guidance provided (for those records of the tables in section 3.4.1 describing missed privacy targets) in the other columns are still useful, once improved, to meet the very privacy targets. The WP29 suggests using that information in the context of a wider and more granular approach to the privacy targets (see also considerations at the end of section 2.2.2 of this Opinion) in order to give guidance on how to meet them. This could be represented either in a tabular form, or, maybe better, in a dedicated section where guidance can be given also in the context of risky processing operations (such as profiling or decisions made on individuals based on automated processing operations).

Risk calculation/prioritisation

Clearer guidance is present on how to calculate and prioritise risks. Better wording and more clarity in the risk calculation section (2.5.1.3) is needed.

Risk treatment

"2.6.1. Risk Modification: implemented and planned controls" should be integrated in "2.5. Step 5 - Data protection risk assessment", and taken into account in the first risk estimation. But the title should not mention "risk modification", which is one of the risk treatment options. It could simply be called "Implemented and planned controls". Then, in "2.6. Step 6 - Identification and Recommendation of controls and residual risks", and especially in "2.6.2. Risk Treatment" additional controls are determined and risks are estimated again as residual risks.

In Opinion 04/2013 the WP29 remarked that no matching existed in the first version of the Template between the risks to be mitigated and the list of possible controls in Annex II. The WP29 welcomes that in the new version of the Template the description of the objective of the possible controls often includes the type of risks it is generally meant to mitigate. Furthermore the non-exhaustive list of generic threats in section 3.4.1 links these threats to the possible controls in Annex II.

Residual risks

For a balanced weighing of the residual risks for at the end of the risk management process it is equally important to identify all the interests at stake at an early stage. These can be drawn from the overall company risk management process, if this exists. Not only economic or other legitimate interests can be represented, but also other stakes such as e.g. social responsibility or compliance with other legal requirements.

The WP29 suggests that a new section be added in order to identify the stakes of the processing. This section could be located between 2.3.1 and 2.3.2 and be called "2.3.2. Stakes of the processing". It should ask for a description of the opportunities of the creation of the smart grid pocessing (marketing / economic, societal, legal compliance, etc.).

An evaluation of the residual risks given the stakes could be added, after the first paragraph of "2.6.4. Resolution". This paragraph might explain that the resolution consists in deciding to accept or not the residual risks given the stakes identified in 2.3.

2.3.2 Roles and responsibilities

The WP29 welcomes the integration (section 1.4.2) of a list of the different types of smart grid operators, including a generic description of the purposes they might process personal data for.

The existence of the specific subsection 2.1.2 now better highlights the need for a clear allocation of controller and processor responsibilities. The example in the text of controllership and possible processor responsibilities in a smart meter should be integrated by other examples tackling more complex situations. A further example is reported in the text (micro grid operator and insurance company involved) where the problem statement exists but no guidance is provided.

Furthermore, as already suggested in Opinion 04/2013, 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 (where a corresponding form already exists in section 3).

2.3.3 The Template forms

Besides other considerations in other sections of this Opinion, the WP29 wishes to underline some other shortcomings in the sections describing some forms to be used to implement the DPIA.

For example, in section 3.3, the relationship among different templates used for smart grid systems identification, characterization and description, the sequence of use of those templates and how exactly they should be used is not clear. There is a reference to an external document without any comment on what the reference is for. Or, there seems to be no reference in the methodology on when the form in section 3.3.5 needs to be used.

On the other hand, a table with primary and corresponding supporting assets is important in guiding the risk assessment.

In general more guidance should be provided on the use of the forms. Having one or more examples in an annex would be very useful.

2.4 Sector-specific content in the DPIA template

One of the main issues in the Opinion 04/2013 was that the risks and controls outlined in the first version of the Template did not reflect industry experience on what the key concerns and best practices are.

The WP29 notes and welcomes that some specific content has been added in the non-exhaustive list of generic threats reported in section 3.4.1.1, in particular under the column whose header is "Specific Energy industry examples of supporting asset vulnerabilities". Still the WP29 believes that some improvement and some more guidance are needed, both in the text and in the template, and especially in order to meet the privacy targets (see also section 2.2.2).

As reminded in section 1.1, the Commission rejected the WP29's proposal to integrate the Best Available Techniques (BATs) deliverable the EG2 is working upon into the Template reportedly because of their scope limited to smart meters and their evolutive nature.

The WP29 confirms its view that the considering the BATs as a deliverable inherently linked to the Template would enable an organisation conducting a DPIA to choose the adequate measures if necessary. The BATs evolutive nature does not counter its complementary role to the DPIA Template. Furthermore, the Template itself will need a review cycle to maintain and refine the methodology after a first phase of application, and anyhow periodically. The fact that the BATs' scope is limited to smart meters and thus not exhaustive is not a reason to exclude its use within a DPIA exercise either. Smart meters represent the subsystems where personal data are mainly collected and processed and in any case it is better to have some guidance than none. Moreover, the WP29 takes this opportunity to suggest that the Commission and the industry explore the possibility to extend the valuable BATs work also to the wider smart grid scope.

In Opinion 04/2013, and specifically in Annex II, the WP29 recommended that at least the most common privacy enhancing technologies ('PETS') and other 'best available techniques' for data minimization would be described briefly and in a technologically-neutral manner in the DPIA Template, and then be further detailed, in the accompanying BAT document. This has not happened. The WP29 still believes that this would be very useful for the industry to both have a portfolio of measures ready to implement and be more aware of what privacy enhancing technologies are so as to design further adequate controls.

2.5 Need for testing/validation of the DPIA template

The WP29 suggests that an adequate certain testing/validation of the DPIA Template be carried out, on the field on the basis of the existing version, and taking as much as possible account of the above comments. The WP29 suggests that following these test, the template and its methodology should be reviewed and enhanced in the light of those experiences and taking into account the aforementioned comments. These test cases, on which WP 29 should be informed and in which individual DPAs may

consider offering some support, can also be useful to provide valuable examples to be included in the Template annexes for a better understanding of the methodology proposed.

2.6 Other considerations

2.6.1 The concept of personal data

Section 2.1 describes how to determine whether personal data are processed in the smart grid subsystem under analysis. The WP29 takes note that the classification as personal data in the examples listed appears to be correct, even though the justification given to identify a piece of information as personal data is not always strictly applying the legal terminology.

E.g. what are called "usage data" are considered personal data because "they provide insight in the daily life of the individual", whereas they are personal data just because they relate to the individual owning the contract and his/her possible family. The fact that they provide insight in the daily life constitutes a privacy impact. This consideration is valid also for the other items listed therein. While the list of examples is certainly helpful for potential users of the template, the impression that such considerable privacy impact is required for data to be considered personal. Furthermore, it should be clear that the list of examples is not exhaustive.

2.6.2 Other remarks on data protection terminology

In some sections the template uses terminology such as "system owner" which is meaningful in the field of application, but does not always clarify the relationship to the DP terminology that may be applicable (such as data controller,…) (p14, 18, 32,…) or about "the individual", "the consumer", the "customer" without clear link to data subject (pages 10, 15,…).

Furthermore, some language used such as "agreed with the customer" (p 10), "customers must have the choice" (p 11) could be matched with the need of obtaining "consent " as defined in article 2(h) of the Directive.

The WP29 invites to consider indicating the relevant data protection terminology as well and to explain the level of interoperability of the terms, where applicable.

2.7 Conclusions and recommendations

The WP29 recognises the work carried out by the EG2 group and realises that the second version of the template constitutes considerable improvement with respect to the previous version insofar as the methodology is better outlined and actionable. Nonetheless, there is still a series of unclear elements and a need for more clarity in some parts, which, if addressed as indicated, will contribute in a determinant way to the successful deployment and use of the template.

The WP29 understands that the version it assessed may still be subject to linguistic and legal editing.

The WP29 is aware of the urgent needs for a DPIA in the industry sector and welcomes a prompt final version of the Template, whose effectiveness, after a certain

period of use, will certainly need to be verified and improved. It recommends therefore to organise a test phase with some real cases on which WP 29 should be informed and in which individual DPAs may consider offering some support, and which should also contribute to ensure that the template provides improved data protection to individuals in the context of the deployment of smart grids. When testing the template and as foreseen in it, industry is encouraged to pay attention to key concepts of the data protection reform, such as data protection by design and by default, data minimisation, the right to be forgotten and data portability.

Furthermore, the WP29 continues to recommend considering the opportunity of defining a generic DPIA methodology from which field specific efforts could benefit.

Done at Brussels, on 4 December 2013

For the Working Party
The Chairman
Jacob KOHNSTAMM

Annex: Additional methodological tools

In "3.5. Step 5 - Data Protection Risk Assessment", the following table could be used to assess the feared events:

Process and personal data	Level of identification (LI)	Feared events	Potential impacts	Prejudicial effects (PE)	Severity (LI+PE)
[list of personal data involved]	[the most appropriate level in the LI scale, based on personal data]	[feared event]	[list of potential consequences on data subjects if the feared event occurs]	[the most appropriate level in the PE scale, based on potential impacts]	[addition]

When personal data are not assessed globally, those lines have to be repeated (e.g. for each process).

The same table could be augmented by other columns corresponding to the threats, so that to be able to show the entire risks:

Process and personal data	Level of identification (LI)	Feared events	Potential impacts	Prejudicial effects (PE)	Severity (LI+PE)	Main threats	Vulnerabilities (VUL)	Risk sources	Capabilities (CAP)	Likelihood (VUL+ CAP)

A new section should be added in order to demonstrate the compliance to the privacy targets. This section could be located between 2.6.2 and 2.6.3 and be called "2.6.3. Compliance with the privacy targets". Since those privacy targets are mandatory and not negociable, it should state that, for each of the privacy targets, the way it is implemented should be described, or a justification for not having implemented it should be provided[9].

The following table could be used for that purpose:

Privacy targets	Explanations	Description / justification
Safeguarding quality of personal data	Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on explicit consent, contract,	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]

[9] This is comparable to the notion of "statement of applicability" in ISO/IEC 27001.

Privacy targets	Explanations	Description / justification
	legal obligation, etc.	
Legitimacy of processing sensitive personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner. Implementation of the right to be forgotten and the right to data portability should be encouraged	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially in the case of profiling.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Safeguarding confidentiality and security of processing	Preventing unauthorized access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured. Breach notification procedure should be promoted	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured. DPIA shall be considered as a determinant tool for this target	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Compliance with data retention requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Privacy by design	Having regard to the state of the art and the cost of implementation, technical and organisational measures and procedures shall be designed both at the time of the determination of the means for processing and at the time of the processing itself in such a way that they fully respect privacy and data protection rights of the data subject.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]
Privacy by default	Mechanisms shall be implemented for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage.	[description of the way the privacy target has been implemented, OR justification if it has not been implemented]

Of course each of the entries above can be multiplied to further break down each of the privacy targets if useful. E.g. "data quality" wraps many other principles like data minimisation and avoidance, necessity and proportionality with respect to the

purposes etc. Furthermore, different controls used to meet the same privacy target might deserve different entries so as to stand out.

This way, in conclusion, data protection risks are managed (assessed and treated), and what is done to comply with the privacy targets is described (and can be controlled).

A mixed approach is still possible, by studying also the risks of missing some privacy targets (not only security but also, e.g. purpose limitation, necessity and proportionality, data retention, granting data subject's rights, etc.).