# Tool Support for Data Protection Impact Assessment in the Smart Grid

Ewa Piatkowska, Agron Bajraktari, Dharini Chhajed, and Paul Smith

AIT Austrian Institute of Technology, Vienna, Austria
{firstname.lastname}@ait.ac.at

**Abstract.** The smart grid promises to enable novel energy services, supporting a greater integration of renewable energy sources. Major issues in this context are data protection and privacy risks, wherein malicious actors or organizations misuse personal data that is collected, processed and stored to enable these services. To address this problem, the European Commission has proposed a risk-driven process to data protection impact assessment. In this article, we introduce this process and present a tool that can support its implementation.

**Keywords:** Smart grid · Privacy · Risk Assessment · Data Protection Impact Assessment

## 1 Introduction

The smart grid will enable new energy services that support so-called prosumers as they monitor and optimise their energy consumption and production. These services can help to efficiently use the energy that is generated by distributed energy resources, such as photovoltaics, allow more precise grid management and control, and enable advanced demand-response schemes. Collecting high-frequency consumption and generation data supports more accurate demand-response strategies, as more reliable forecasting and accurate profiling can be be achieved.

However, collecting personal data, such as high-frequency consumption measurements, can result in significant data protection and privacy risks, revealing information about a person's behaviour in the most privacy sensitive place, the home. The possible consequences of these risks include price discrimination, profiling for targeted marketing, compromises of household security (i.e., burglary based on knowledge about a householder's presence), and fraud.

To support the assessment and mitigation of these risks, the European Commission has proposed a Data Protection Impact Assessment (DPIA) template for smart grid and smart metering systems [6]. It is proposed that the use of the template will enable smart grid stakeholders, such as Distributed System Operators (DSOs), reduce data protection and privacy risks, and support them as they realize their obligations under the new General Data Protection Regulation (GDPR), which will be enforced in May 2018.

In this article, we introduce the DPIA template and present a tool to support its implementation. In developing the tool, and using it to assess data protection and privacy risks for a number of novel smart grid services, we have made a number of improvements to the proposed DPIA template, and identified where further work is required.

## 2 Related Work

We present a brief introduction to data protection and privacy impact assessment methods; a survey of state-of-the-art approaches is presented by Wright [7].

The Privacy Impact Assessment (PIA) Handbook [3], produced by the Information Commissioner's Office (ICO) in the UK, defines a PIA process, providing guidance on how each step of the process can be implemented. Two types of process are proposed in the Handbook – a *full*, detailed and comprehensive assessment, and a *small-scale*, less-formal analysis. In addition, the Handbook provides a list of screening questions that can be used to determine what form of assessment should be undertaken. More recently, the ICO has defined a PIA code of practice [4], which describes a six-step summary of a PIA process. The steps that are defined, including defining information flows and risks that could result in an impact to privacy, clearly influenced the DPIA template that has been advocated for the smart grid.

These ICO documents propose general, i.e., not technology-specific, privacy impact assessment approaches. In contrast, the European Commission has proposed data protection impact assessment processes for specific technologies. Initially, a DPIA template for radio-frequency identification (RFID) applications was proposed [2]. The RFID DPIA framework was largely developed by industry representatives, and was endorsed by the Article 29 Working Party[1] in February 2011 [1]. Unfortunately, the framework has not been well-received or widely-used. The user community has highlighted a lack of technology-specific guidance related to risks and controls. At a later stage, the European Commission has developed a similar guidance for smart grids, which we summarize next. For a high-level assessment of the suitability of this guidance, we refer the reader to work by Kloza *et al.* [5]

## 3 The Data Protection Impact Assessment Template for Smart Grids

The Expert Group (EG) 2 of the Smart Grid Task Force (SGTF) has proposed a *Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems* [6]. The aim of the template is to support smart grid stakeholders,

[1] The Article 29 Working Party consists of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission.

such as Distribution System Operators (DSOs), perform a DPIA. The implementation of a DPIA is necessary under the new EU General Data Protection Regulation (GDPR), which will come into force as law in May 2018. The template has been subject to a review process, with a new version expected to be released in early 2017. In what follows, we summarize the proposed template, based on the version from March 2014 (the version that was under review)[2].

The assessment process that is defined in the template is organized into a number of steps, in a similar manner to the ICO PIA code of practice [4]. Initially, a pre-assessment step is used to determine whether there is a need to conduct a DPIA for a smart grid service. The decision is made based on the results from a series of questions. For example, if the system includes services that involve personal data, such as a website that allows a consumer to monitor their energy consumption, then a DPIA is required. Subsequently, in an initiation step, the service owner defines the team that will implement the assessment and any necessary resources, such as documentation. It is intended that this team is multi-disciplinary, containing a data protection officer, persons with knowledge of the system under consideration, and third-parties to support the process.

Following these initial steps, information about the smart grid system is collected, including relevant use cases, information flows, and a description of the underlying infrastructure such as components and communication interfaces. The expected outcome of this exercise is to collect all of the information assets that are considered *personal*, such as energy consumption data. In the DPIA template, such assets are called *primary assets*, which are processed, stored or transmitted using *supporting assets* – computers and network equipment, for example.

With an understanding of the system, relevant risks are identified. In this context, risks are defined as *feared events*, which represent an undesirable situation with respect to a data subject's personal data, e.g., illegitimate access, and the threats that might result in a feared event. Having identified the risks, they are assessed in terms of the impact of feared events and the likelihood of associated threats manifesting. In Sec. 4, we describe how these values are determined in the context of our DPIA tool.

The next step is to identify and recommend controls and residual risks, which involves developing an appropriate risk treatment strategy and proposing controls or other mitigation strategies to reduce risks to acceptable levels. Moreover, the risk remaining after the risk treatment – the residual risk – needs to be identified. A review and maintenance step ensures the continuous monitoring of risks and the implementation of the risk treatment strategy. Finally, the results of the assessment should be documented.

[2] In discussions with sources involved in the development of the DPIA template, we have learned the overall structure of the process will remain the same in the final version. However, some details about how individual steps should be implemented will change.

## 4 Tool Support for Data Protection Impact Assessment

To support the implementation of a DPIA using the template described in Sec. 3, we have developed a tool. In order to provide a user-friendly interface and to enable teamwork, it has been developed as a web-based application using the Django framework[3]. In this section, we provide an overview of how the tool functions.

Having performed a registration step, access to the tool is authenticated with a username and password. Two different roles exist with associated privileges: the *team leader* – the assessment owner – and a *team member*. The former creates, updates and deletes an assessment, and manages the team members that are assigned to it; the latter can browse or edit the assessment. In line with the template, interaction with the tool starts with a pre-assessment survey. If it transpires that a DPIA is required, documentation that is related to the assessment can be uploaded and assigned to relevant steps of the process.

In the next step, the user (a team leader or member) is tasked with describing the smart grid service under consideration. In the tool, we guide the user to focus on the information flows in each step of a scenario. *Primary assets* – personal data – are identified whilst defining these exchanges, including the data subjects they relate to. In addition, the underlying *supporting assets* for primary asset communication, processing and storage are identified. Supporting assets can be of different types, such as hardware, software or communication equipment – this information is used to automatically shortlist relevant threats in a later stage. Fig. 1 presents how the list of primary and supporting assets are related in the tool, alongside a navigation bar for the whole process.

Subsequently, a risk assessment exercise is performed, which is organized in the tool into three main parts. (We dispensed with the concept of feared events from the DPIA template, but kept the approach to determining likelihood and impact.) First, supporting assets are analyzed for cyber-security vulnerabilities that could be exploited by a threat actor. In addition, relevant threats for each supporting asset are identified from a predefined catalogue, filtered by the type of supporting asset. Second, the *likelihood* of each threat manifesting is assessed using two indicators: *(i)* a level of vulnerability; and *(ii)* the capability of a risk source (threat actor). Third, the *impact* of primary assets being compromised by a threat to a supporting asset is assessed. The impact is determined by evaluating a prejudicial effect and the level of the identification of the data subject. The prejudicial effect is a measure of the severity of the negative consequences to a data subject, if a primary asset is compromised. Meanwhile, the level of identification specifies how readily a data subject can be identified.

For each of the four indicators of likelihood and impact, a value $\geq 1$ and $\leq 4$ is assigned. These values are determined by members of the assessment team, using guidance provided in the DPIA template and the tool. The risk level is calculated as the sum of the likelihood of a threat to a *supporting asset*

[3] Django is a Python framework that supports the rapid development of web-based applications: https://www.djangoproject.com/.

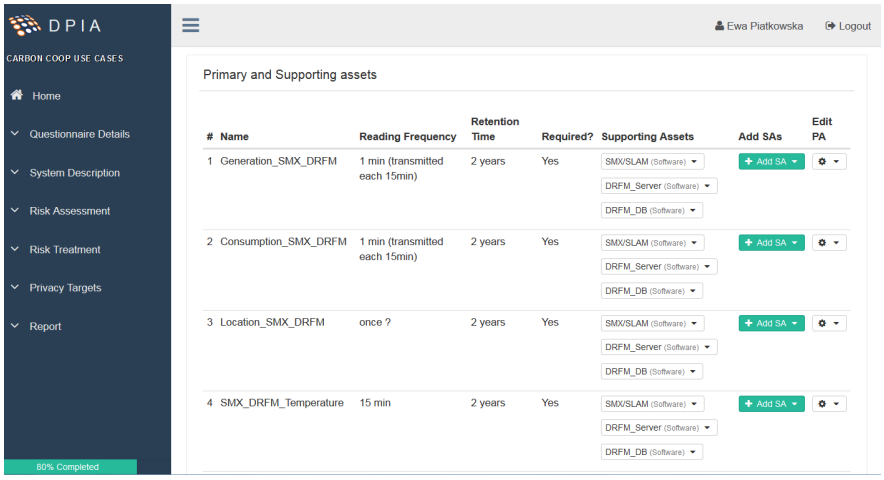


**Fig. 1.** A screenshot of the DPIA tool, showing a list of primary and supporting assets

(of a primary asset), and the impact of a compromise of a *primary asset* on a data subject. The relationships between supporting assets and threat likelihood with primary assets and impact, which are used to determine a risk level, are automatically maintained by the tool. In a following step, the assessed risks are presented to the user, ranked by their level, to support risk evaluation and risk treatment.

We have introduced a new step to assess the implementation of high-level privacy targets and to verify that an organization is respecting data subjects' rights. In contrast to the previous assessment, which focuses on cyber-security-related data protection issues, this step is intended to determine whether an organization is operating a smart grid service in a privacy preserving manner. The user selects high-level privacy targets – from a catalogue provided by the DPIA template – that are relevant to the service under scrutiny, e.g., related to the legitimacy of processing sensitive data. Subsequently, they are asked to identify all the privacy threats that could jeopardize the selected privacy targets, and to suggest controls to ensure the implementation of these targets, e.g., creating a privacy policy or certifying the processing of the data to be more transparent.

Finally, having completed all of the previous steps, the tool can generate a report in PDF format that can be downloaded. The report presents a summary of the service description, the risk assessment results, and proposed risk treatment strategies. It is intended this report can be submitted to a national data protection authority to support compliance with the GDPR.

## 5 Conclusion and Outlook

In this article, we have introduced the Data Protection Impact Assessment (DPIA) template for smart grid and smart metering systems, and a tool to

support its implementation by a smart grid stakeholder. There are a number of useful features that our tool provides: *(i)* direct support for distributed team working; *(ii)* access to guidance about how to implement each step of the DPIA process that is embedded directly in the tool; *(iii)* hints about the nature of the required input, using interface elements such as tooltips; *(iv)* pre-selected relevant content to support analyses (e.g., threats that relate to asset types); and *(v)* the automatic generation of documentation to support compliance with the GDPR. Collectively, these features should make the implementation of a DPIA more straightforward, therefore requiring less effort.

In developing our tool, we departed from the draft process that is proposed in the DPIA template in two major ways. First, we removed the concept of feared events – in the original template, risk treatments mitigate feared events, resulting in reduced traceability regarding how risk treatments address the likelihood and impact of specific threats. Second, a set of specific privacy impact assessment steps have been introduced. These steps support organizations evaluating whether a smart grid service is implemented in a compliant and privacy preserving manner, and is less concerned with data protection from malicious adversaries.

We have applied the tool as part of our ongoing work in the EU-funded Nobel Grid project[4], which is developing novel smart grid services. In doing so, we have identified a number of areas for further work. For example, it appears, when assessing the level of identification that is associated with primary assets, considering combinations of sets of assets (e.g., consumption data, device identifiers, and geo-location of installations) is important. This is because they may collectively reveal more information about a data subject or make it more trivial do so. Additionally, in many cases, these data items are communicated and stored together, and share the same fate given a cyber-attack. Therefore, considering distinct levels of identification for each primary asset, in isolation, could result in a misplaced sense of risk and the development of inadequate risk treatment strategies. Addressing this issue, and others that we have identified in a series of DPIA workshops, will steer our future work.

## Acknowledgements

This research has been conducted within the Nobel Grid Project, funded from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 646184.

## References

1. Article 29 Data Protection Working Party: Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (2011). URL `http://ec.europa.eu/justice/`

[4] The Nobel Grid Project: http://nobelgrid.eu/

data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf
2. European Commission: Privacy and Data Protection Impact Assessment Framework for RFID Applications (2011). URL http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
3. Information Commissioner's Office (ICO): Privacy Impact Assessment Handbook, Version 2.0 (2009)
4. Information Commissioner's Office (ICO): Conducting Privacy Impact Assessments, Code of Practice (2014). URL https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
5. Kloza, D., Dijk, N.V., Hert, P.D.: Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies, pp. 11–47. Elsevier (Syngress), Waltham, MA (2015)
6. Smart Grid Task Force 2012-14 Expert Group 2: Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems (2014). URL https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf
7. Wright, D.: The state of the art in privacy impact assessment. Computer Law and Security Review **28**(1), 54–61 (2012)