2018

An Evaluation Framework for Privacy Impact Assessment Methods

Konstantina Vemou
University of the Aegean, Greece, kvemou@aegean.gr

Maria Karyda
Dept. of Information and Communication Systems Engineering, University of the Aegean, mka@aegean.gr

AN EVALUATION FRAMEWORK FOR PRIVACY IMPACT ASSESSMENT METHODS

Research full-length paper

Track N° 11 - Security and Privacy

Vemou, Konstantina, University of the Aegean, Greece, kvemou@aegean.gr

Karyda, Maria, University of the Aegean, Greece, kvemou@aegean.gr

Abstract

Privacy Impact Assessment (PIA) methods guide the implementation of Privacy-by-Design principles and are provisioned in the European Union's General Data Protection Regulation. As implementing a PIA is still an intricate task for organizations, this paper provides a critical review and assessment of generic PIA methods proposed by related research, Data Protection Authorities and Standard's Organizations. The evaluation framework is based on a comprehensive set of criteria elicited through a systematic analysis of relevant literature. This paper also identifies elements of PIA methods that require further support or clarification as well as issues that still remain open, such as the need for implementation of supporting tools.

Keywords: privacy impact assessment, privacy risks, evaluation criteria, GDPR.

1 Introduction

Privacy Impact Assessment (PIA) is a risk management approach that has emerged primarily in order to identify and mitigate privacy risks imminent in new systems (Clarke, 2009) and to implement the principles of Privacy-by-Design (Oetzel and Spiekermann, 2014), so as to foster citizens/consumers' trust (Wright and Hert, 2012). Several legal frameworks mandate its conduction, such as Canada's Privacy Act and (EC) 2016/679, the European Union's General Data Protection Regulation (also known as EU GDPR), while, Data Protection Authorities (DPAs) worldwide have emphasized the importance of implementing PIAs and have published high level guidelines on conducting them (e.g. UK ICO, 2014; Canada TBS, 2010); the International Organization for Standardization (ISO 2017) recently published a PIA guidelines standard (ISO/IEC 29134).

Conducting a PIA remains a complicated and bewildering task for organizations processing personal data, mainly due to the lack of guidance on how to carry out such an assessment (Meis and Heisel, 2015; Berendt et al. 2017; Van Puijenbroek and Hoepman, 2017; De and Le Metayer, 2017), as well as due to the plethora of methods available. While several methods and guidelines have been published by Data Protection Authorities, they follow different approaches and provide limited assistance on how to organize a PIA project. Currently, however, Privacy-by-Design, the idea of enhancing privacy to Information and Communication Technology (ICT) systems from the very start of their inception or design (Cavoukian, 2010), becomes a basic requirement for ICT systems processing Personally Identifiable Information (PII), and online providers from all over the world offering their services to millions of EU citizens (European Commission, 2015) need to comply with EU GDPR.

This paper addresses this issue, by analysing current PIA methods and providing an evaluation framework to organizations. With this framework, PIA practitioners are supported in selecting the PIA method that best suits their needs (special legal framework, needs for PIA project organization guidance, etc.). We also identify critical issues that require more analysis or research to allow effective implementation of PIA methods.

In the next section, relevant literature on PIA methods evaluation is critically analysed; section 3 describes the research method followed, along with evaluation criteria derived. Section 4 presents evaluation findings and conclusions and issues for further research are presented in section 5.

2 Evaluating PIA Methods: the Current Landscape

Although the basic concept of a PIA method dates back to 2009 (Clarke, 2009) and many methods and guidelines have been proposed since then, little work on comparing and/or evaluating these methods has been published. Relative research mainly includes PIA guidelines proposed by privacy protection authorities and is out of date, due to the constant update of proposed guidelines and methods. An example of the latter is the UK PIA Code of Practice published by the information Commissioner's Office (ICO) in 2014, replacing the respective Privacy Impact Assessment Handbook of 2009.

The first research evaluating PIA guidelines was conducted in 2011 by Clarke (2011) who evaluated PIA guidelines published by Commissioner Offices of Canada, Australia, etc. The evaluation criteria mainly focused on the document's quality, such as its discoverability, applicability to regions or industry sections, making clear that responsibility for PIA lies within the organization and orientation on completing a report template versus the risk analysis process. Other criteria used included: obligatory status and timing of the PIA, protected privacy dimensions, applied legal frameworks, stakeholders' engagement, incorporation of the PIA process in corporate mechanisms, e.g. project funding, and the role of the oversight agency. Clarke's evaluation highlighted best practices of PIA guidelines published at that time and showed that some guidelines limited PIAs by proposing legal compliance checks or failed to convey the importance of stakeholders' engagement.

In the context of the European Commission (EC)-funded project PIAF, a, Wright et al. (2013) argued on the necessity of the EU to establish its own framework of PIA conduction and performed a comparative evaluation of several countries' guidelines (including Australia, Canada, Ireland, New Zealand, UK and USA) to identify best elements/practices that could be employed. Criteria used for this evaluation focused on the context of PIA implementation, such as its potential obligatory status (mandated by law) and whether the guidelines provide arguments in favour of undertaking a PIA. Other criteria focused on the quality of the PIA method and on provided assistance, such as addressing different privacy aspects (informational, bodily, territorial, locational, communications), examining the necessity of PIA conduction in an introductory step, external stakeholders consultation, proposing the PIA report structure, assigning PIA accountability to senior management, review of the PIA report by an external authority and highlighting need for PIA updates throughout the lifecycle of a project.

Towards the same direction, Wadhwa and Rodrigues (2013) proposed an evaluation tool grading PIA reports, called the PIA Evaluation and Grading System (PEGS). This tool applied quantitative evaluation criteria on PIA conduction steps, derived from the PIAF project. Criteria were weighted according to their contribution towards a successful PIA conduction and included: clarification of early initiation, identification of who conducted PIA and publication of the PIA report (weight=1), project description, purpose and relevant contextual information, information flow mapping, legislative compliance checks and identification of stakeholder consultation (weight = 2), identification of privacy risks and impacts, identification of solutions/options for risk avoidance and mitigation, and recommendations handling after the PIA (weight = 3).

Notario et al. (2015) evaluated the privacy impact assessment methods proposed in the EU (Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU) and Privacy and Data Protection Impact Assessment Framework for RFID), in the context of the EU-funded project PRIPARE (Preparing Industry to Privacy by Design by supporting its Application in Research). Evaluation criteria included the existence of supporting questionnaires extracted from legal frameworks to ensure a project's legal obligations are met, examination of the privacy impact from the organization perspective (financial losses) or the individual perspective (identifiability and sensitivity of personal data), the metrics used to measure privacy risks, and the proposal of risk mitigation strategies.

Focusing on the implementation of PIA projects, van Puijenbroek and Hoepman (2017) evaluated PIA practices followed by 15 organizations in the Netherlands, in order to investigate whether they resulted in privacy-friendly products and systems. Their study, although based on descriptive answers by Data Protection Officers (DPO) or executives with equivalent roles, indicated that PIAs were conducted mainly from the perspective of the data controller, instead of the data subject which would be affected, that controls were mainly chosen to mitigate rather than avoid privacy risks and that PIAs were not repeated, as should have been the case, throughout the product or system development process.

Currently, several PIA methods of diverse origin (e.g. proposed by academics, Data Protection Authorities, etc.) are available, many of which have been recently updated. This paper provides a framework for evaluating proposed guidelines and identifies issues that require further support or clarification to facilitate their implementation.

3 Research Method

Through a systematic analysis of relevant research and publications on PIA methods we have derived a set of criteria (presented in Table 1), which are used to evaluate available PIA methods (included in Table 2), with regard to the process followed, as well as the guidelines provided to PIA conductors. Criteria were formed so as to evaluate whether PIA methods adequately provide a) guidance to organizations through the important steps of PIA (e.g. sign-off of the report), b) supporting material for PIA practitioners (e.g. guidance in risks identification, PIA report templates) to facilitate PIA conduction, c) guidance on organizing a PIA project (e.g. assigning responsibilities, selecting PIA team members and involving external stakeholders), so as to provide effective implementation guidelines throughout the entire life-cycle of a PIA project.

No	Criterion description
1	Is there a step to determine whether a PIA is necessary (threshold analysis)?
2	Is a specific legal framework used as a reference for defining privacy targets?
3	Does the process assess risks for the company (apart from ones for the individual)?
4	Is structured guidance (e.g. in the form of steps etc.) to assist in risk assessment provided?
5	Is any part of the process supported by automated tools?
6	Are organizational and technical measures to treat risks included/proposed?
7	Are directions for PIA conduction during Information Technology/ Information Systems (IT/IS) development included?
8	Is the entity responsible for organizing the PIA project specified?
9	Is guidance on setting up the PIA team provided?
10	Does it involve external stakeholders' consultation during risk assessment?
11	Is guidance on identifying external stakeholders provided?
12	Is the entity responsible for signing-off of the PIA report specified?
13	Is an external evaluation/audit of the PIA report required?
14	Is publication of the PIA report to inform external stakeholders provisioned?
15	Is the owner of residual risks specified?
16	Are periodical reviews provisioned? Are revision thresholds defined?
17	Is a PIA report template proposed? Which are its contents?

Table 1. *Evaluation criteria*

To identify available PIA methods and guidelines, we searched for «"privacy impact assessment" method» in «Google Scholar», since 2009, when Clarke formally cited PIA as a systematic process for evaluating the potential effects on privacy of a project.

The set of derived PIA methods included academic papers as well as policy-oriented papers, published from Data Protection Authorities around the world (e.g. the UK's Information Commissioner Office), in their latest version. We have analysed PIA methods regardless of whether they were policy-driven or academic and regardless of their focus on a certain legal framework (e.g, EU GDPR, Canada Directive on PIA), but have excluded PIA methods targeted for specific industries or technologies, such as RFID (Spiekermann, 2012) and Smart Grids (Smart Grid Task Force 2012-14 Expert Group 2, 2014). The following methods (selected based on their references) were finally analysed (Table 2).

Method title	Type/Origin	Description
Systematic PIA methodology	Academic	Based on the German Federal Office for Information Security (BSI) risk method. (Oetzel and Spiekermann, 2014)
Data Protection Impact Assessment (DPIA) process under EU GDPR	Academic	A process to conduct PIAs, operationalizing established requirements from the EU GDPR. (Bieker et al., 2016)
UK PIA Code of practice	Policy-based / DPA	Published by the UK's Information Commissioner Office. It includes lists of risks and questionnaires to guide the analysis. (UK ICO, 2014)
New Zealand PIA toolkit	Policy-based / DPA	Proposed by the Office of Privacy Commissioner of New Zealand. It includes a template for PIA reports and examples of risk mitigation examples. (OPC New Zealand, 2015)
Australian ICO PIA guide	Policy-based / DPA	Proposed by the Office of the Australian Information Commissioner. It includes a compliance check with the principles of Australia's Privacy Act (1988). (OAIC, 2014)
CNIL PIA method	Policy-based / DPA	Proposed by the French Commission Nationale de l'Informatique et des Libertes (CNIL), based on EBIOS security risk management method. It is accompanied by a beta version of a tool to guide steps of PIA. (CNIL, 2018)
Canada Directive on PIA	Legal framework	Issued by the government of Canada in 2010, mandates PIAs for federal projects and services. It contains an appendix with guidance on PIA conduction and assessing risks for personal data handling. (Canada TBS, 2010)
Privacy Impact Assessment Framework (PIAF) methodology	Academic	The outcome of an EC-funded project, which reviewed PIA methodologies published until 2012 and proposed an "optimized" PIA. (Wright, 2013)
ISO 29134	Standard	A standard issued in 2017 to guide practitioners on PIA conduction. (ISO, 2017)

Table 2. *PIA methods evaluated*

4 Evaluation Framework and Analysis of Available PIA Methods

The methods we analysed (see Table 2 above) comprised of similar steps such as a step to decide whether a thorough PIA is necessary, threats identification, selection of risk treatment options and documentation, while they differed in provision of supporting material to carry out these steps, in roles and responsibilities assignment, etc.

Risk identification

Our analysis identified that in many cases structured guidance for risks identification (questionnaires/matrices or lists of risk examples) is based on specific legal frameworks (Canada TBS, 2010; Bieker et al., 2016; OAIC, 2014; OPC New Zealand 2015). This practice, although allows organizations achieve compliance in specific legal contexts, may mislead PIA practitioners and limit their view on privacy risks emerging from the PII processing. Also, while all methods identify privacy risks for individuals, only a subset of them identify risks for the organization that resulted of personal data processing (Oetzel and Spiekermann, 2014; UK ICO, 2014; Canada TBS, 2010; OPC New Zealand,

2015). Furthermore, only a few provide metrics for the risk assessment (Canada TBS, 2010; ISO, 2017; OPC New Zealand, 2015).

Risk Treatment Controls

Available PIA methods provide privacy controls at different detail levels to mitigate risks. While some provide high-level (general), organizational controls (including Oetzel and Spiekermann, 2014; UK ICO, 2014; Bieker et al., 2016; OAIC, 2014), other propose specific technical controls (OPC New Zealand, 2015; CNIL, 2018). What is more important though, is that only a few emphasize the need to eliminate privacy risks instead of treating them, by reconsidering the data process and deciding not to process some data elements if not critical for the desired purpose (UK ICO, 2014; ISO, 2017).

PIA report templates

Most of the methods analysed provide PIA report templates to assist practitioners, with the following identified as key information to be recorded: system/project owner and description, information flows and processing purposes, privacy risks, privacy controls to mitigate risks, action plan for recommendations implementation and sign-off information. Other contents of PIA reports, although not proposed in all methods include: methodology used for PIA conduction, reasoning behind the selected controls, owner of the residual risks and description of stakeholders' consultation plan. Respectively, most methods recognize the potential need to publish the PIA report and highlight the need to obscure confidential information in published reports, but with minimum guidance on which information to exclude.

Tools automating the PIA process

With the exception of CNIL's beta version of PIA software, available methods make no reference to any tools that can automate the PIA process or create a PIA report.

Organization of PIA projects

In terms of organizing a PIA project, most of the methods analyzed refer to the person who organizes a PIA, without however clearly defining his/her role and responsibilities. For instance, Oetzel and Spiekermann (2014) and CNIL (2018) propose PIA conduction by the Data Protection Officer, Bieker at al. (2016), Wright (2013) and OAIC (2014) assign the responsibility to the Project's Manager (PM) and ISO (2017) to either one of them. Also, guidance on mapping PIA steps (or its iterations) to specific project phases is provided in only a few of the examined methods (Oetzel and Spiekermann, 2014; UK ICO, 2014). Furthermore, no guidelines are provided on selecting PIA team, except by UK ICO (2014), OAIC (2014) and OPC New Zealand's (2015).

Similarly, responsibilities for signing-off the PIA report and assuring implementation of proposed controls are not included in most of the examined methods although the need for identifying for such roles is implied in PIA report templates (UK ICO, 2014; ISO, 2017; OAIC, 2014; OPC New Zealand, 2015). Also, responsibility for PIA periodical reviews as well as related thresholds are only implied, but not explicitly described in available methods.

Furthermore, some methods provide the option of an external sign-off, e.g. by Data Protection Authorities (Canada TBS, 2010; ISO, 2017; OAIC, 2014; OPC New Zealand, 2015), or an independent third party (Bieker et al. 2016; Wright, 2013).

External stakeholders

With regard to involving external stakeholders in risk assessment, such as privacy advocates and consumer representatives, all analysed methods identify this need as optional but useful and most provide general guidance for their identification. However, only a few provide guidance on how to set-up consultation plans with external stakeholders (Bieker et al., 2016; ISO, 2017).

Conclusively, while comprising of similar steps, available PIA methods adopt different approaches on implementation. Furthermore, our analysis identified areas in which partial or no guidance is provided,

	1- Threshold Analysis	2- Legal Frame-work	3- Risks for Organi-zation	4- Guidance for Risk Assessment	5- Automation Tool	6- Proposed Controls	7- Map in IT/IS Development Phases	8 – PIA Responsible	9- PIA Team Skills
Systematic PIA methodology	X	X	✔	Privacy targets' examples, Impact perspectives	X	General	✔	X	X
DPIA process under EU GDPR	✔	EU GDPR	X	X	X	General	X	PM	X
UK PIA Code of practice	✔	X	✔	Screening questions, risks and treatment strategies examples	X	General	✔	DPO/ Risk Manager	✔
New Zealand PIA toolkit	✔	New Zealand's Privacy Act 1993	✔	Questionnaire to guide risk identification, metrics for risk assessment	X	✔	General	X	✔
Australian ICO PIA guide	✔	Australia's Privacy Act 1988	X	Questionnaire to guide Risk identification	X	General	X	PM	✔
CNIL PIA method	X	EU GDPR	X	Template guiding PIA, metrics to assess impact of risks, threat examples, list of controls	YES (BETA tool)	✔	X	Project Owner	X
Canada Directive on PIA	✔	It is itself a law	✔	Metrics to assess impact, list of legal requirements	X	X	X	Senior Execu-tive responsible for the project	X
PIAF methodology	✔	X	X	X	X	X	X	PM	X
ISO 29134	✔	X	✔	Metrics to assess risk impact and likelihood, examples of privacy risks	X	ISO 27001 and ISO 29151	X	Responsible for PII protection / PM	X

Table 3. *Evaluation Framework and Analysis (Criteria 1-9)*

	10 – External Stakeholders Involvement	11- External Stakeholders Identification	12 – PIA Sign-off Role	13 – External Audit of PIA Report	14- PIA Report Publication	15- Accountable for Treatment Plans Implementation	16- Periodical Reviews	17- PIA Report Template
Systematic PIA methodology	Optional	X	X	X	✔	X	✔	✔
DPIA process under EU GDPR	✔	✔	X	By independent third party and the DPA	✔	X	✔	✔
UK PIA Code of practice	✔	✔	Senior Management/ PM	X	✔	X	During project	✔
New Zealand PIA toolkit	In complex projects	General	X	Audit by DPA only if required by law	✔	Someone in the project or within the organisation's governance framework	✔	✔
Australian ICO PIA guide	✔	✔	X	Audit by DPA only if Privacy Act allows	✔	Project Manager and the organization	✔	✔
CNIL PIA method	Only in validation phase	X	Role not determined	X	✔	Role not Determined	✔	✔
Canada Directive on PIA	X	X	Senior Officials/ Executives/ Legal Services Unit	Typical review by Treasury Board and DPA (public organizations)	✔	Approval from the Minister	✔	✔
PIAF methodology	✔	✔	Role not determined, CEO held accountable	By external companies or the International Association of Privacy Professionals	✔	Project Manager and the organization	✔	X
ISO 29134	✔	✔	Responsible for the project	Audit by DPA if required by law	✔	Risk Owner (and management by signing acceptance statement)	✔	✔

Table 4. *Evaluation Framework and Analysis (Criteria 10-17)*

thus need further support, such as external stakeholders' consultation and assigning roles and responsibilities for PIA conduction. The Evaluation Framework and results of the evaluation are depicted in Tables 3 and 4.

5 Conclusions and Further Research

In this paper we analyse nine commonly used PIA methods and evaluate the guidelines they provide to organizations. The evaluation framework we provide is based on a comprehensive set of criteria and assists PIA practitioners in selecting guidelines that best suit their needs. For instance, methods using the legal framework applying to the organization, to extract privacy targets, could be preferred by PIA practitioners. Also, methods providing guidelines on selection and involvement of external stakeholders could be selected by organizations developing systems that highly impact certain categories of data subjects and are in need to involve them in the PIA project. The proposed evaluation framework assists academics and DPAs by revealing issues that are currently not adequately described, including PIA roles and responsibilities assignment and assistance to PIA practitioners in terms of supporting tools and templates.

The analysis identified steps in which guidance is provided by most methods, such as threshold analysis, risk identification and PIA report preparation; however, we also identified different approaches in guidelines, including risk identification. Analysing available methods we have identified practices that play an important role for the success of PIA projects. For instance, exploring privacy risks from the organization perspective contributes towards a holistic view of the risks induced and provokes a more diligent effort to treat or prevent privacy risks. Also, eliminating privacy risks instead of treating them, by reconsidering the data process and deciding not to process some data elements if not critical for the desired purpose should be espoused, to accomplish Privacy-by-Design. For this reason, PIA methods should directly propose reviewing the list of involved personal data in each risk mitigation cycle.

On the other hand, we critically endorse provision of privacy controls' lists as practical guidance in generic PIA methods. As some technologies would be suitable in certain cases of processing and not suitable in some others and there is also a risk of providing obsolete technical controls, due to rapid advances of technology, PIA practitioners could be misled by provided controls lists. However, providing privacy controls' examples could be useful in the rationale of conducting a PIA for a specific business area (e.g. bank sector, smart grids) or technology (e.g. RFID). For this reason, apart from evaluating the remaining generic PIA methods identified from literature review, we plan to also evaluate PIA methods focusing on specific technologies or business areas.

Furthermore, in the context of high-level, generic PIA methods, we have identified unnecessary steps documenting the need for DPAs to audit the PIA report, as responsibility to sign-off a PIA report still lies within the organization and the role of Data Protection Authorities is highly dependent on each organization's legal context. Dependence on specific legal frameworks is also imminent in the risks identification phase of many methods, which provide supportive questionnaires or risk examples based on data protection laws. Such guidance, while assisting to PIA practitioners should be critically used, as it limits applicability of PIA methods in different jurisdictions and poses the risk of limiting the scope of PIA to data protection, thus neglecting the effects of a process on other aspects of the person's everyday life (by privacy threats such as surveillance and decisional interference). Also, if used exclusively, such guidelines could distract PIA practitioners from conducting a risk analysis and mislead them into performing a legal compliance check.

Gaps and differences identified in this research should be taken into account to propose an optimised PIA method. For instance, such a method should provide organizations with a detailed method of identifying privacy risks and metrics to evaluate them, along with examples of risks to explain its application. Also, guidance on how to embed legal requirements in such a method should be provided. In addition, there is need to propose an organizational scheme, in order to practically guide PIA practitioners in organizing PIA projects.

This research also identifies areas that need to be further analysed by researchers and DPAs publishing PIA methods, such as guidance on selecting the PIA team, in terms of specific skills related to each

task in the PIA cycle. Further information on how to engage the most representative external stakeholders in each PIA step (consultation plan) should be provided, with special information on how to distinguish risk perceptions from actual risks (ISO, 2017).

Another area that needs further research is the implementation of tools to support PIA conduction. For instance, tools to automate risk identification from data flows, to automatically create the PIA report as a result of the risk assessment steps or to manage communication and collaboration with external stakeholders could be implemented to assist PIA practitioners.

References

Berendt, B., Littlejohn, A., Kern, P., Mitros, P., Shacklock, X., Blakemore, M. (2017). "Big data for monitoring educational systems". Publications Office of the European Union, Luxembourg.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M. (2016). "A process for Data Protection Impact Assessment under the European General Data Protection Regulation". In: Schiffner S., Serna J., Ikonomou D., Rannenberg K., (eds.) Proceedings of the Annual Privacy Forum 2016. Privacy Technologies and Policy. Lecture Notes in Computer Science, vol 9857, p. 21, Springer, Cham.

Cavoukian, A.(2010). "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian" Ph.D. Identity in the Information Society 3(2), 247-251.

Clarke, R. (2009). "Privacy impact assessment: Its origins and development." Computer law and security review 25(2), 123-135.

Clarke R. (2011). "An Evaluation of Privacy Impact Assessment Guidance Documents." International Data Privacy Law 1(2), 111-120 (2011).

Commission Nationale de l'Informatique et des Libertes (CNIL) (2015). "Privacy Impact Assessment (PIA) Methodology" URL: https://www.cnil.fr/en/PIA-privacy-impact-assessment-en (visited on 2018/04/22).

De, S.J., Le Métayer, D. (2017). "A Refinement Approach for the Reuse of Privacy Risk Analysis Results". In: *Annual Privacy Forum*, pp. 52-83. Springer, Cham.

European Commission (2015). "Special Eurobarometer 423 Cyber Security", Report 978 DR-01-15-143-EN-N, European Commission.

International Organization for Standardization (ISO) (2017). "ISO/IEC 29134 Information technology – Security techniques — Privacy impact assessment – Guidelines".

Meis, R., Heisel, M. (2015). "Supporting privacy impact assessments using problem-based privacy analysis". In: International Conference on Software Technologies, pp. 79-98. Springer, Cham.

Notario, N., Crespo, A., Martín, Y.S., Del Alamo, J.M., Le Métayer, D., Antignac, T., Wright, D. (2015). "PRIPARE: integrating privacy best practices into a privacy engineering methodology." In: Security and Privacy Workshops (SPW), 2015 IEEE, pp. 151-158. IEEE.

Oetzel, M.C., Spiekermann, S. (2014). "A systematic methodology for privacy impact assessments: a design science approach." European Journal of Information Systems 23(2), 126-150.

Office of the Australian Information Commissioner (OAIC) (2014). "Guide to undertaking privacy impact assessments" URL: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments (visited on 2018/03/02).

Office of the Privacy Commissioner (OPC) New Zealand (2015). "Privacy Impact Assessment Toolkit", URL: https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/ (visited on 2018/03/02).

Smart Grid Task Force 2012–14 Expert Group 2 (2014). "Data protection impact assessment template for smart grid and smart metering systems" URL: https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf (visited on 2018/03/02).

Spiekermann, S. (2012). "The RFID PIA–developed by industry, endorsed by regulators." Privacy impact assessment, Springer Netherlands, 323-346.

Treasury Board of Canada Secretariat (Canada TBS) (2010). "Directive of Privacy impact assessments" URL: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308 (visited on 2018/03/02).

UK Information Commissioner's Office (ICO) (2014). "Conducting Privacy Impact Assessments: Code of Practice" URL: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (visited on 2018/03/02).

van Puijenbroek, J.P.M., Hoepman, J.H. (2017). "Privacy Impact Assessments in Practice: Outcome of a Descriptive Field Research in the Netherlands". In: Ceur Workshop Proceedings, Alamo, J.M. del (ed.), IWPE 2017: International Workshop on Privacy Engineering: Proceedings of the 3rd International Workshop on Privacy Engineering, co-located with 38th IEEE Symposium on Security and Privacy (S&P 2017) San Jose (CA), USA, May 25, 2017, pp. 1-8.

Wadhwa, K., Rodrigues, R. (2013). "Evaluating privacy impact assessments." Innovation: The European Journal of Social Science Research 26(1-2), 161-180.

Wright, D. (2013). "Making privacy impact assessment more effective." The Information Society 29(5), 307-315.

Wright, D., Hert, P. (2012). "Introduction to privacy impact assessment". Privacy Impact Assessment, Springer Netherlands, 3-32.

Wright, D., Finn, R., Rodrigues, R. (2013). "A comparative analysis of privacy impact assessment in six countries." Journal of Contemporary European Research 9(1).