PIAF
PRIVACY IMPACT
ASSESSMENT FRAMEWORK

A step-by-step guide to privacy impact assessment

David Wright & Kush Wadhwa[1]

Presentation paper for the second PIAF workshop, Sopot, Poland, 24 April 2012

A privacy impact assessment (PIA) should be regarded as a process. It is not just about preparing a report, although a report helps document the process. It is a process that focuses on identifying the impacts on privacy of any new project, technology, service or programme and, in consultation with stakeholders, taking remedial actions to avoid or mitigate any risks. The process should start when a project is in the early planning stages, when there is still an opportunity to influence the project's design or outcome[2]. The process should carry on throughout the project's life. New risks may emerge as the project progresses, and they should be assessed whenever they become apparent.

There are differences in PIA methodologies and processes. Based on research funded by the European Commission, the PIAF consortium has drawn on the best elements of existing methodologies and processes and formulated the main steps in the PIA process as follows:

1. Determine whether a PIA is necessary (threshold analysis)

Generally, if the development and deployment of a new project (or technology, service…) impacts upon privacy, the project manager should undertake a PIA. The impacts may be minimal or great and wide-ranging. A threshold analysis (see Annex 1) can help determine whether a PIA is necessary and the scale of the PIA. A PIA should be undertaken when it is still possible to influence the design of a project or, if the project is too intrusive upon privacy, the organisation may need to decide to cancel the project altogether rather than suffer from the negative reaction of consumers, citizens, regulatory authorities, the media and/or advocacy gadflies.

2. Identify the PIA team and set the team's terms of reference, resources and time frame

The project manager should be responsible for the conduct of a PIA, but she may need some additional expertise, perhaps from outside her organisation. Depending on the estimated scale of the PIA, the project manager or the privacy impact assessor may need to form a team to undertake the PIA. The team could bring together expertise from information security experts, lawyers, operations managers, ethicists, public relations experts, the chief privacy officer, etc. As the PIA progresses, the assessor may find that she needs still other expertise. The project manager and/or the organisation's senior management should decide on the terms of reference for the PIA team, its budget and its time frame. The assessor may come under considerable pressure to complete the PIA quickly so as not to delay the project, but she may need to resist compromising the integrity and adequacy of her PIA mission and may need to ensure she has the full support of the organisation's CEO and/or its management board. The terms of reference should spell out whether public consultations are to be held, to whom the PIA report is to be submitted, the budget for the PIA, the time frame, whether the PIA report is to be published. The terms of reference should make clear that the PIA is a process and

[1] Trilateral Research & Consulting, London, www.trilateralresearch.com

[2] This is effectively the definition of a privacy impact assessment. A project should be understood in its widest sense, i.e., including a technology under development or a product or a service in the planning stage or a programme or other initiative still in the drafting or design stage.

that the process will need to continue beyond preparation of the PIA report. If the assessor's work or that of an external consultant comes to an end with publication of the report, the project manager and/or the organisation's CEO and/or management board should decide how implementation of recommendations will be monitored and who will be responsible for the monitoring and what factors will determine whether the PIA report needs to be updated.

3. Prepare a PIA plan

The assessor should prepare a plan for conducting the PIA. She can prepare the PIA plan using this PIA process document, but may need to tailor it to the exigencies of the project to be assessed. The plan should spell out what is to be done to complete the PIA, who on the PIA team will do what, the PIA schedule and, especially, how the consultation will be carried out. An important part of the plan should address consultation. It should specify why it is important to consult stakeholders in this specific instance, who will be consulted and how they will be consulted (e.g., via public opinion survey, workshops, focus groups, public hearings, online experience…).

4. Determine the budget for the PIA

Once the project manager and/or assessor have prepared a PIA plan, they can estimate the costs of undertaking the PIA and seek the budgetary and human resources necessary from the organisation's senior management. Unfortunately, the assessor may be constrained in what she can do in the PIA by the budget allocated by the organisation. If the assessor is unable to do an adequate PIA, she should note this in her PIA report. The assessor may need to revise her PIA plan based on the budget available.

5. Describe the proposed project to be assessed

The assessor should describe the project or technology or service to be assessed. As the development of the project or technology or service may still be at an early stage, there may not yet be that much known about the project. The assessor can update the description as more becomes known. The description can be used in at least two ways – it can be included in the PIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (why is the project being undertaken, how it fits in with the organisation's other services or product lines, who comprises the target market, how it might impact the consumer-citizen's privacy, what personal information will be collected, whether other organisations offer a competitive service offering). The project description should state who is responsible for the project. It should indicate important milestones and, especially, when decisions are to be taken that could affect the project's design.

6. Identify stakeholders

The assessor should identify stakeholders, i.e., those who are or might be interested in or affected by the project, technology, service. The stakeholders could include people who are internal as well as external to the organisation. They could include regulatory authorities, customers, citizen advocacy organisations, suppliers, service providers, manufacturers, system integrators, designers, academics and so on. The assessor should identify these different categories and then identify specific individuals from within each of the category, preferably as representative as possible. The full range of stakeholders may not be immediately apparent to the assessor. Some stakeholders may only become apparent as the PIA progresses. If necessary or useful, they too should be brought into the consultation process. The range and number of stakeholders to be consulted should be a function of privacy risks and the assumptions about the frequency and consequences of those risks and the numbers of consumer-citizens who could be impacted. Thus, the number of stakeholders to be consulted could be quite limited if the project or service is also expected to be small, e.g., the project or service might involve only employees of a small or medium-size enterprise.

7. Analyse the information flows and other privacy impacts

Although seven different types of privacy have been identified[3], undoubtedly the most common privacy risks are those that involve the use of personal data or personally identifiable information (PII). Thus, the assessor should consult with others in the organisation and perhaps external to the organisation to describe the information flows and, specifically, who collects what information from whom for what purpose and how does the organisation use the collected information, how is the information stored, secured, processed and distributed (i.e., to whom does the organisation pass on the information, for what purpose and how well are secondary users (e.g., the organisation's service providers, apps developers) protecting that information or do they pass it on to still others? This analysis should be as detailed as possible as it will be of significant help in identifying potential privacy risks.

The project manager or assessor should prepare a briefing paper on the information flows and the impacts on different types of privacy. This briefing paper, like that describing the project, should form part of the PIA report. It should also be made available to the stakeholders to be consulted, so that they have as adequate understanding of the information flows and privacy impacts as possible.

8. Consult with stakeholders

The project manager and/or privacy impact assessor should consult with as many stakeholders as appropriate or possible (taking into account the available budget). There are many reasons for doing so, not least of which is that they may identify some privacy risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream – when the project or technology or service is deployed – an adequate consultation at an early stage may help the organisation avoid or minimise liability. Furthermore, consulting stakeholders may provide a sort of "beta test" of the project or service or technology. Consulted stakeholders are less likely to criticise a project than those who were not consulted.

There are several different ways of consulting stakeholders and the assessor should consider which will be most appropriate in the circumstances. The assessor or other members of the PIA team could interview stakeholders directly. They could convene workshops of experts or stakeholder representatives. They could hold focus groups of ordinary consumer-citizens. They could conduct surveys by telephone or e-mail or face to face. They could post the project description on the organisation's website and invite comments. They could hold public hearings where they describe the project and invite comments from the audience or from experts and then invite comments after the experts have spoken. They could prepare stories or adverts in the media and invite comments from readers. They could conduct a Delphi survey of experts, to query them on potential privacy risks now and in the future.[4]

9. Check the project complies with legislation

A privacy impact assessment is more than a compliance check, nevertheless, the assessor or her legal experts should ensure that the project complies with any legislative or regulatory requirements. The

[3] Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2013 [forthcoming].

[4] For a longer list of possible techniques, see OECD, Stakeholder Involvement Techniques, ISBN 92-64-02087-X, Paris, 2004, pp. 30-32 [Box 2. Commonly cited techniques for informing deliberation through stakeholder involvement].

assessor should not assume that if the project complies with the Data Protection Act (or Directive or Regulation), all is well. There will be several (or more) legal texts to be taken into account, and if she takes into account the seven types of privacy as well as ethical principles and surveillance issues, there could many laws and regulations that need to be taken into account. Although the Opinions of the Article 29 Data Protection Working Party do not have the force of law or regulation, nevertheless the prudent project manager would be well advised to take the Opinions into account.

10. Identify risks and possible solutions

The assessor and her PIA team, preferably through stakeholder consultation, should identify all possible risks, who those risks will impact and assess those risks for their likelihood (frequency) and consequence (magnitude of impact) as well as the numbers of people who could be affected. In addition to the annexes of this guide, there are several publications which are helpful in identifying and assessing possible risks.[5] Assessing risks is a somewhat subjective exercise. Thus, the assessor will benefit from engaging stakeholder representatives and experts to have their views. Deciding how to mitigate or eliminate or avoid or transfer the risk is also a somewhat political decision as is the decision regarding which risks to retain. The assessor or project manager or organisation may decide that the benefits of the project or technology outweigh the perceived risk arising from its development and deployment. The organisation should maintain a risk register, wherein the assessor (and/or other organisation employees) identify the risks, their seriousness, what the organisation has decided (if anything) to do about the risk, who is the risk "owner" (who is responsible for managing it). The risk register should be regularly updated (e.g., every six months).

Privacy risk management should be regarded as part of the organisation's risk management. In some countries, e.g., the UK, companies listed on the stock exchange are obliged to state in their annual reports what risks face the organisation and how the organisation is managing those risks. Privacy risks should be included in such annual reports. In doing so, the organisation can avoid charges that it was wilfully negligent in informing shareholders and regulatory authorities about the (privacy) risks facing the organisation.

11. Formulate recommendations

Based on her analysis of the privacy risks and impacts, the assessor should prepare a set of recommendations, which will form part of the PIA report. The assessor should be clear to whom her recommendations are directed – some could be directed towards different units within the organisation, some to the project manager, some to the CEO, some to employees or employee representatives (e.g., trade unions), to regulatory authorities, third-party apps developers, etc. The assessor should provide the rationale for each of her recommendations. The recommendations could include procedural and more general organisational matters, e.g., relating to training and raising awareness and accountability, as well as those relating specifically to privacy risk management.

12. Prepare and publish the report, e.g., on the organisation's website

The assessor should prepare her PIA report, and the organisation should publish it on its website. In some countries, the data protection authority (DPA) or privacy commissioner (PC) expects organisations to complete a PIA report according to a specified format or template, and may want to

[5] Highly recommended are Stoneburner, Gary, Alice Goguen and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, MD, July 2002; International Organization for Standardization (ISO), *Information technology — Security techniques — Information security risk management*, ISO 27005, Geneva, 15 June 2008; European Network and Information Security Agency (ENISA), EFR Framework Introductory Manual, Heraklion, 2010.

see the report or even to comment on the adequacy of the report.[6] Some organisations may be afraid to publish their PIAs because they fear negative publicity or they have concerns about competitors learning something they don't want them to. Such concerns seem overdone. Publication offers many benefits and opportunities to the organisation. It demonstrates that the organisation treats privacy seriously, and consequently its customers or citizens. Customers and citizens are more likely to invest their trust in an organisation that treats their privacy with respect. It offers an opportunity to gather additional feedback from stakeholders. It offers the organisation an opportunity to distinguish itself from its competitors.

Government agencies in the US are obliged to publish their PIAs and do so without apparent damage.

For organisations concerned about publishing commercially sensitive information or security sensitive information, there are solutions. The organisation can simply redact the sensitive bits or put them into a confidential annex.

US government agencies list their published PIAs on each agency's webpage. Thus, for example, at the Department of Homeland Security's PIA webpage, one can find dozens of PIAs listed.[7] British Colombia and Alberta each have registries of PIAs.[8]

13. Implement the recommendations

The project manager and/or the organisation do not need to accept all these recommendations, but they should say which recommendations they have implemented already or intend to implement and which they do not intend to implement and the reasons why they do not intend to do so. The organisation's response to the assessor's recommendations should be posted on the organisation's website. This transparency will show that the organisation treats the PIA recommendations seriously, which in turn should show consumers and citizens that the organisation merits their trust.

The organisation should put in place a mechanism or system for updating the PIA report as necessary and, especially, for monitoring the implementation of the recommendations.

The DPA / PC may in some instances also wish to see that the organisation is implementing the PIA report recommendations.

14. Third-party review and/or audit of the PIA

Existing PIA reports are of highly variable quality, from the thoughtful and considered to the downright laughable. Some PIA reports exceed 150 pages, others are only a page and a half in length, the sheer brevity of which makes them highly suspect. While organisations should extract the maximum value from a PIA – in terms of identifying privacy impacts and risks and dealing with them

---

[6] For example, in accordance with section 69(5) of the British Columbia's Freedom of Information and Protection of Privacy Act (FOIPP Act), ministries must complete a PIA using a specific PIA form, which they must submit to the Office of the Information and Privacy Commissioner (OIPC) for review and comment. The OIPC has published a template on its website for preparation of PIAs.
http://www.oipc.bc.ca/public_info/Early_Notice_and_PIA_ProcedureforSubmission%28Mar2012%29.pdf
In Alberta, the Health Information Act (HIA) obliges private sector health care "custodians" (service providers) to submit a PIA for review by Office of the Information and Privacy Commissioner of Alberta. See OIPC, Privacy Impact Assessment Requirements, 2009, p. 10.
http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf. The OIPC also specifies the format for PIAs (see ibid., p. 16 et seq.). Other jurisdictions, while not making a particular PIA format mandatory, do recommend a specific PIA report format or template. See, for example, Ireland's Health Information and Quality Authority, Guidance on Privacy Impact Assessment in Health and Social Care, December 2010, p. 31. http://www.hiqa.ie/resource-centre/professionals

[7] http://ipv6.dhs.gov/files/publications/gc_1282922720391.shtm

[8] Alberta's registry of PIAs can be found here: http://www.oipc.ab.ca/pages/PIAs/Registry.aspx

at an early stage in order to avoid the downstream costs and embarrassment of having to rectify or cancel a project because its flaws have become apparent to all – some organisations see the PIA as a burden and treat it in the most perfunctory way possible.

Independent, third-party review and/or audits are the only way to ensure PIAs are properly carried out and their recommendations implemented. The Office of the Privacy Commissioner of Canada has indicated and extolled the benefits of independent audits.[9]

15. Update the PIA if there are changes in the project

Many projects undergo changes before completion. Research on technological development may go in several different directions before achieving its goal. Whenever changes occur, the project manager and/or assessor should revisit the privacy impact assessment to see whether it needs to be amended, which will almost certainly be the case where new privacy impacts become apparent that were not previously considered. Depending on the magnitude of the changes, the assessor may need to revisit the PIA as if it were a new initiative, including a new consultation with stakeholders.

16. Embed privacy awareness throughout the organisation and ensure accountability

The chief executive officer (CEO) is responsible for ensuring that all employees are sensitive to the privacy implications, the possible impacts on privacy, of what they or their colleagues do. The CEO should be accountable to her supervisory board or shareholders for ensuring that the organisation does not transgress any privacy or data protection legislation as a minimum and, even if it does not, for ensuring that the organisation acts in a way that would not trouble citizens or consumers. The CEO should "sign off" (be held accountable for) the development or deployment of any new technology, project, service, programme or whatever and attest that the new technology, project or whatever does not impact negatively privacy. Before the organisation funds a new initiative, it should consider whether a PIA is necessary.

[9] Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience", in David Wright and Paul De Hert, *Privacy Impact Assessment*, Springer, Dordrecht, 2012.