PIAF

A **P**rivacy **I**mpact **A**ssessment **F**ramework
for data protection and privacy rights

Grant Agreement
JUST/2010/FRAC/AG/1137 – 30-CE-0377117/00-70

Deliverable D3

Recommendations for a privacy impact assessment framework for the European Union

Editors
Paul De Hert, Vrije Universiteit Brussel (VUB)
Dariusz Kloza, Vrije Universiteit Brussel (VUB)
David Wright, Trilateral Research & Consulting LLP (TRI)

Contributors
Kush Wadhwa, Trilateral Research & Consulting LLP (TRI)
Gus Hosein, Privacy International (PI)
Simon Davies, Privacy International (PI)

Prepared for
European Commission – Directorate General Justice

Brussels – London, November 2012

PIAF
PRIVACY IMPACT
ASSESSMENT FRAMEWORK

Executive summary

This deliverable offers recommendations with regard to policy-making and practice on privacy impact assessments (PIAs). These recommendations are split into two sets. The first set is addressed to policy-makers intending to develop a PIA policy in their jurisdictions or improving existing ones. This part analyses the rationale and methods of introduction of a PIA policy, identifies and describes the constitutive elements of a PIA and discusses the role of data protection authorities (DPAs) in the process of PIA. The second set of recommendations is addressed to the assessors actually carrying out PIAs for whom the guidance on the best practice is offered.

Contents

Executive summary 2

1. Introduction 5

1.1. Overview of the concept of PIA 5
1.2. Background to the PIAF project 6
1.3. Purpose and scope of this deliverable 6

2. Recommendations for PIA policy 7

2.1. Introduction of PIA policy 7
2.1.1. High-level support for PIA 7
2.1.2. Compulsory nature 7
2.1.2.1. Rationale 7
2.1.2.2. Means of introduction 7
2.1.2.3. Red tape 9
2.1.3. Legal basis 9
2.1.4. Harmonisation 10
2.1.5. Conflicts of interest 10
2.1.6. Multi-organisation and trans-border dimension 11
2.1.7. Relation to prior checking 12
2.2. The core PIA elements 12
2.2.1. An on-going process 12
2.2.2. Scalability 13
2.2.3. All privacy types 13
2.2.3.1. Privacy vs. data protection 13
2.2.3.2. Beyond PIA 15
2.2.3.3. Terminology 15
2.2.4. Accountability 16
2.2.5. Transparency 17
2.2.5.1. Stakeholders' involvement 17
2.2.5.2. Publication of the PIA report 19
2.2.5.3. Central public registry 20
2.2.5.4. Sensitive information 20
2.2.6. Risks management and legal compliance check 20
2.2.7. Audit and review 21
2.3. Leadership of the data protection authorities 21

3. Recommendations for PIA practice 23

3.1. PIA environment and infrastructure 23
3.1.1. Internal architecture 23
3.1.2. Privacy awareness 23
3.1.3. Professional independence of the assessor 23
3.2. Preliminary issues 24
3.2.1. Threshold analysis 24
3.2.2. Determination of the scale and scope of PIA 26
3.2.3. Roles and responsibilities 26
3.3. The PIA process 27
3.3.1. Early start 27
3.3.2. Project description 27
3.3.2.1. General description of the project 27
3.3.2.2. Information flows and other privacy implications 28

3.3.3. Stakeholders' consultation 28
3.3.3.1. Identification 28
3.3.3.2. Information 29
3.3.3.3. Consultation 29
3.3.3.4. Consideration 29
3.3.4. Risks management 30
3.3.4.1. Risks assessment 30
3.3.4.2. Risks mitigation 30
3.3.5. Legal compliance check 31
3.3.6. Recommendations and report 31
3.3.7. Decision and implementation of recommendations 32
3.3.8. Audit and review 32
3.4. PIA is a living instrument 32
4. Bibliography 33

1. Introduction

1.1. Overview of the concept of PIA

A privacy impact assessment (PIA) is a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative (hereinafter: project) and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts.

The concept of PIA has been known since the mid-1990s and has become progressively more common. The growing interest in PIA is caused by the robust development of privacy-invasive tools, by a belated public reaction against the increasingly privacy-invasive actions of public authorities and corporations and by a natural development of rational management techniques.[1] A PIA is considered to be one of the right tools to address these and other information society challenges.

From a historical perspective, the first guidance documents on PIAs were released after 1998. The UK Information Commissioner's Office published a PIA handbook in 2007 and revised it in 2009.[2] The Resolution of the 31st International Conference of Data Protection and Privacy Commissioners, held in Madrid in 2009, calls for a PIA too.[3] In the United States, PIAs became mandatory by virtue of Sec 208 of the E-Government Act of 2002.[4] In 2008, ISO developed a standard for a PIA in financial services.[5]

However, a PIA is a concept still "under construction", particularly in Europe. One of the turning points in PIA development in Europe, due to its scale and complexity, was the endorsement of the European Union's (EU) Radio-Frequency Identification (RFID) PIA framework by the Art 29 Working Party in February 2011.[6] Following this experience, a data protection impact assessment (DPIA) framework is being developed for smart metering systems.[7] The next turning point was the proposal for the new General Data Protection Regulation, released on 25 January 2012.[8] In its Art 33, the proposed Regulation explicitly provides for a DPIA.

---

[1] Clarke, Roger, „Privacy Impact Assessment: Its Origins and Development", *Computer Law and Security Review*, Vol. 25, No. 2, April 2009, pp. 123-135. http://www.rogerclarke.com/DV/PIAHist-08.html

[2] Information Commissioner's Office, *Privacy Impact Assessment Handbook*, Version 2.0, June 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

[3] Cf. Art 22(f) of the *International Standards on the Protection of Personal Data and Privacy* ("the Madrid Resolution"), Madrid, 4-6 November 2009. http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf

[4] E-Government Act of 2002, Pub.L. 107-347, 44 USC 36. http://www.gpo.gov:80/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[5] International Organization for Standardization, *ISO 22307:2008. Financial services – Privacy impact assessment*, 2008. http://www.iso.org/iso/catalogue_detail?csnumber=40897

[6] *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, Brussels, 12 January 2011. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

[7] European Commission, *Recommendation on preparations for the roll-out of smart metering*, Brussels, 9 March 2012, COM(2012) 1342 final.

[8] The EU data protection reform package consists of two proposals: one for the "General Data Protection Regulation" and the other for the "Police and Criminal Justice Data Protection Directive". The latter contains no requirement of PIA; Art 26 of the draft Directive calls on the Member States to ensure that controllers in the police and justice sector consult the supervisory authority prior to the processing of certain types of personal data. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, 25 January 2012, COM(2012) 11 final; European Commission, *A proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Brussels, 25 January 2012, COM(2012) 10 final.

1.2. Background to the PIAF project

PIAF (*A Privacy Impact Assessment Framework for data protection and privacy rights*) is a European Commission co-funded project that aims to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and to the processing of personal data.[9]

The 22-month project included, in its first phase, a review of privacy impact assessment policies and practices in Australia, Canada, Hong Kong, Ireland, New Zealand, the US and UK to identify which elements may be used effectively to construct a model framework applicable to the EU. The first deliverable was published in September 2011. In the second phase, the partners concluded empirical research with regard to factors that affect the adoption of a PIA policy in the EU Member States, which led to the second deliverable, published in August 2012. Both phases concluded with workshops (one in Brussels on 12 October 2011 and another in Sopot, Poland, on 24 April 2012) where the findings were presented and discussed.

The PIAF partners followed these developments with recommendations to the European Commission and the EU Member States as well as to organisations carrying out PIA, i.e. as reflected in the present and final deliverable. In addition to these deliverables, the consortium partners have presented the project's findings at numerous third-party workshops and conferences and prepared several papers in scholarly publications, listed in the bibliography (cf. 4 below).

1.3. Purpose and scope of this deliverable

This deliverable builds upon the two previous deliverables, i.e. the first, on the review of PIA policies and practices in seven countries and the second, on the factors affecting the adoption of a PIA policy in the EU Member States, as well as upon academic papers, the experience of the editors and correspondence between editors and stakeholders. It attempts to provide recommendations for the best PIA policy and practice for the European Union.

This deliverable contains three main chapters. In Chapter 2, we provide our recommendations for policy-makers who might be developing a new PIA policy in their jurisdiction, or improving an existing one, while in Chapter 3 – for those actually carrying out PIA – we offer guidance on the best practice. This is a follow-up of the structure proposed by Wright and De Hert.[10] The editors are well aware that this distinction is not a perfect one as some issues might overlap. These two sections discuss the best practice identified in the first deliverable and are contrasted with the concerns of data protection authorities, if any, identified in the second deliverable. Finally, chapter 4 lists a bibliography of academic papers produced in relation to the PIAF project.

The contents of this deliverable are the sole responsibility of the editors and can in no way be taken to reflect the views of the European Commission.

Editors welcome comments and suggestions at paul.de.hert@vub.ac.be, dariusz.kloza@vub.ac.be and david.wright@trilateralresearch.com, respectively.

[9] The PIAF project's website can be found at http://www.piafproject.eu.
[10] Wright, David and Paul De Hert, "Findings and Recommendations", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, p. 445.

2. Recommendations for PIA policy

2.1. Introduction of PIA policy

2.1.1. High-level support for PIA

A PIA policy needs high-level support of policy-makers, regulators and private sector.

The introduction of a PIA policy within a jurisdiction greatly depends on the support of high-level policy-makers and regulators (government) as well as their counterparts in private sector (business). These stakeholders need to encourage a PIA policy too.

However, the introduction of impact assessment procedures may be treated by politicians and officials as an unwelcome or even "pointless" extra burden on their time and resources.[11] In order to successfully introduce a PIA policy, both public and private sectors must be convinced that the benefits of PIA outweigh its disadvantages (cf. 2.1.2.2 below).

2.1.2. Compulsory nature

2.1.2.1. Rationale

There is a strong case for compulsory PIA as there is a fundamental right at stake. A PIA should be mandatory, at least when there is a likelihood of risk to the protection of privacy and personal data.

Both rights – to privacy and to data protection – enjoy in Europe the status of fundamental rights (cf. Art 8 European Convention on Human Rights (ECHR) and Arts 7-8 of the Charter of Fundamental Rights of the European Union (CFR)). A PIA is a means to ensure enjoyment of these rights. Furthermore, compromising privacy might result in irreparable harm for the individual. Therefore, as a minimum, a PIA should be mandatory for projects that are likely to present risks to the protection of privacy and personal data. Yet the regulator should encourage organisations to perform a PIA whenever the project impacts on privacy and personal data (cf. 3.2.1 below).

Unless a PIA is mandatory, many organisations may not undertake them, even though their projects might have serious privacy and data protection impacts. As Bayley and Bennett argue, the likelihood of PIAs being conducted is related to the degree of policy compulsion to conduct them and to accountability for their completion.[12] Thus, the choice of the method to introduce a PIA policy impacts the level of protection.

2.1.2.2. Means of introduction

There should be a legal obligation to carry out a PIA. The compulsory nature of PIA should be strengthened by proportionate sanctions for non-compliance. A PIA could be tied to budget submissions. However, this should not preclude other incentives for carrying out a PIA being identified and communicated to organisations, in particular, the benefits of PIA.

A PIA policy should be mandated by law (cf. 2.1.3 below). Organisations should be accountable for completing a PIA (cf. 2.2.4 below). Proportionate sanctions of an administrative nature

[11] Parker, David, "(Regulatory) Impact Assessment and Better Regulation", in Wright and De Hert, p. 81.
[12] Bayley, Robin, and Colin Bennett, "Privacy Impact Assessments in Canada", in Wright and De Hert, p. 182.

should be foreseen for non-compliance, intentionally or negligently, with the obligation to carry out a PIA.

As a way to ensure that the public sector actually does perform a PIA, in Canada and the United States, PIAs are tied to budget submissions. In Canada, government institutions must complete and forward a PIA to the Treasury Board of Canada Secretariat to accompany submissions for funding new programs and projects, and in the United States, government agencies must include a PIA with submissions to the Office of Management Budget. In the private sector, an organisation should have procedures in place whereby funding for the proposed project is tied to completion of a satisfactory PIA beforehand. For example, if an organisation plans a new project for which board approval is required, then a PIA should accompany the submission to the board. Nevertheless, the PIA report may need to be revised and the PIA process may need to continue as the project is developed (cf. 2.2.1 below and 3.4 below).

However, a number of additional inducements have been identified to convince organisations to carry out a PIA. By contributing to efficient project and business practices, a good PIA can bring advantages such as:

- Internally:
  - management of risk (identification and mitigation), as well as evidence thereof;
  - enhancement of informed decision-making – by obtaining a direct and credible source of information and by enhancing internal communication;
  - early warning system – by spotting potential privacy problems and taking effective countermeasures;
  - avoidance of inadequate solutions, i.e. better balance between conflicting interests; if the privacy impacts are unacceptable, the project may even have to be cancelled altogether;
  - avoidance of unnecessary costs, i.e. providing cost-effective solutions, since it is less expensive to build privacy by design into a project at an early stage than to take remedial actions after a project has commenced, thus reducing the risk of having to terminate or substantially modify a project after its implementation in order to comply with privacy and data protection requirements;[13]
  - avoidance of sanctions and a possible waiver of civil liability;[14]
  - improving security of a project;
  - imposing the burden of proof for the harmlessness of a project on the organisation initiating or seeking to initiate the project;
  - education and raising awareness about privacy among employees;
  - providing "corporate memory", i.e. ensuring that the information gained during the project can be shared with future PIA teams and others outside the organisation;
  - repository for information requests from public authorities and customers;
- Externally:
  - strategic advance, i.e. demonstration of compliance with privacy and data protection legislation and confirmation that an entity takes privacy seriously, as privacy is a core corporate value;

[13] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 463.

[14] Gellert, Raphaël and Dariusz Kloza, "Can privacy impact assessment mitigate civil liability? A precautionary approach", in Erich Schweighofer et al. (eds.), *Transformation juristischer Sprachen. Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012*, Österreichische Computer Gesellschaft, Wien, 2012, pp. 497 – 505.

- competitive advantage, i.e. businesses and organisations able to sustain a high level of good will, trust and confidence from customers and citizens can differentiate themselves from their rivals;
- improving public awareness;
- understanding the perspectives of stakeholders;
- avoidance of negative public reaction, of loss of trust and of reputation;
- gaining public trust towards the project or technology deployed.

Finally, a "privacy culture" within an organisation (cf. 3.1 below) increases substantially the likelihood that PIAs would be actually carried out.

2.1.2.3. Red tape

A mandatory PIA should be balanced against a policy to reduce red tape. It should provide for a simple and pragmatic tool.

Opponents of PIA could criticize it as an unnecessary cost, adding to the bureaucracy of decision-making and as something that will lead to delays in implementing a project. There is a risk that if a PIA policy were too burdensome for organizations, it would be performed perfunctorily, i.e. like a "tick-box" exercise and it would thus be less effective than e.g. audit practices carried out voluntarily. Some authorities, while backing a compulsory instrument, believe that it should nevertheless depend on the sector (e.g. administration), size (e.g. big companies) and/or threshold conditions, i.e. risks involved in data processing (e.g. sensitive data).

The very need for most organisations is the availability of practical and pragmatic tools to conduct a PIA, which do not require a long introduction.[15] In particular, a firm legal environment as well as clear PIA guidelines and PIA templates are of crucial importance here.

2.1.3. Legal basis

At least the core elements of PIA (cf. 2.2 below) should have a firm legal basis.

Worldwide, PIA is mandated either by hard law (a legal statute, e.g. acts of parliament, delegated acts or by-laws) or by soft law (non-binding legal instruments, e.g. recommendations or guidance material). The degree of detail, i.e. how specific such regulation is, varies considerably.[16]

The chosen legal instrument must satisfy certain criteria of quality of law making. The European Court of Human Rights has addressed this issue on numerous occasions, by analysing the concept "in accordance with law" [cf. Art 8(2) ECHR]. Although these deliberations are primarily applicable in case of interference with a fundamental right, the conditions for the quality of law are equally applicable here. For example, in a classical judgement *Olsson v Sweden*, the Court ruled:

> *(…) (a) A norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail; however, experience shows that absolute precision is unattainable and the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are*

[15] We are grateful to Kristine Rytter for this remark.
[16] For a detailed analysis, see Wright, David, Kush Wadhwa, Paul De Hert, and Dariusz Kloza (eds.), *PIAF*: *A Privacy Impact Assessment Framework for data protection and privacy rights*. Deliverable D1. Prepared for the European Commission Directorate General Justice. 21 September 2011, pp. 195-198. http://www.piafproject.eu

vague (see, for example, the Sunday Times judgment of 26 April 1979, Series A no. 30, p. 31, § 49).
(b) The phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law; it thus implies that there must be a measure of protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by, inter alia, paragraph 1 of Article 8 (art. 8-1) (see the Malone judgment of 2 August 1984, Series A no. 82, p. 32, § 67).
(c) A law which confers a discretion is not in itself inconsistent with the requirement of foreseeability, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see the Gillow judgment of 24 November 1986, Series A no. 109, p. 21, § 51).[17]

However, there is a question about how much of a PIA policy should be regulated in a legal statute, how detailed it should be and how much should be left for future regulation, if any, by other means (e.g. soft law). Regulation of only core elements gives a lot of flexibility, i.e. a general model whose content needs to be adjusted depending on the specifics of the case. However, a PIA framework should not be made too complex and complicated, thus risking some legal uncertainty. These core elements are discussed in section 2.2 below.

2.1.4. Harmonisation

A PIA policy should enjoy a minimum level of harmonisation.

The processing of personal data across national borders by both the public and the private sectors has increased exponentially in recent years, as has the need for legal protections for personal data. In order to avoid gaps in protection of privacy and personal data as well as to facilitate the global data flows, there have been calls for harmonisation.[18]

Consistent with foregoing, both the PIA policy and PIA practice (i.e. methodology) should enjoy a minimum level of harmonisation worldwide and in particular in the European Union. However, some flexibility is required to reflect the local conditions as well as the characteristics of specific sectors (e.g. health, RFID or smart metering).

2.1.5. Conflicts of interest

A PIA policy should ensure that a PIA is carried out independently.

In a typical situation, a proponent of a project would engage an assessor and would pay for a PIA. Thus there is a risk of a conflict of interest: the assessor might tailor her findings to the proponent's expectations. Normally a project's proponent would seek a PIA that sanctions the project or at least with a few cosmetic changes.[19]

[17] ECtHR, *Olsson vs. Sweden*, Application no. 10465/83, Judgement of 24 March 1988, § 61.
[18] Kuner, Christopher, "An International Legal Framework for Data Protection: Issues and Prospects," *Computer Law & Security Review*, Vol. 25, No. 4, July 2009, pp. 307–317.
[19] Cf. Edwards, John, "Privacy Impact Assessment in New Zealand – A Practitioner's Perspective", in Wright and De Hert, p. 199; Waters, Nigel, "Privacy Impact Assessment – Great Potential Not Often Realised", in Wright and De Hert, p. 153.

Therefore, it could be argued that a PIA should be carried out by e.g. an internal privacy (data protection) officer, whose independence is sanctioned by law[20] and by appropriate resources at her disposal, or by an external entity whose independence is beyond any doubt (cf. 3.2.3 below). This would insulate the assessor from the pressure involved in a direct relationship with the project's proponent as their client.

However, because of the pressures on the assessor, PIA reports might only hint at potential problems. Assessors trying to fully document adverse privacy effects, or to suggest alternatives or safeguards, but constrained in their ability to do so too bluntly, can often nevertheless include clues that can be detected and interpreted by experienced readers.[21]

2.1.6. Multi-organisation and trans-border dimension

A PIA should be carried out for projects sponsored by more than one organisation as well as for projects with a trans-border dimension, at least if they have significant privacy implications. A PIA policy should facilitate such assessments.

Especially when it comes to information and communications technologies, a growing number of projects are sponsored by more than one organisation, and a growing number of organizations are engaged in projects of a trans-border nature, or a mix thereof. These projects should not escape a PIA.

These projects – perhaps due to their scale – are *more likely* to present risks to the protection of privacy and personal data. They are also likely to present *different* risks, i.e. those not likely to occur in projects that are individual or executed only in a single jurisdiction. Examples of such projects include those involving international transfers of personal data. A significant objective of a PIA in such projects is to ensure that the project meets or exceeds the data protection and privacy requirements in all the relevant jurisdictions and achieves a level of trust amongst consumers and regulators.[22]

Transnational PIAs have attracted some attention in the corporate world. The international consultancy Deloitte & Touche published a guide to a cross-border privacy impact assessment as long ago as 2001, although aimed at companies with cross-border operations rather than government agencies.[23] More recently, a PIA has been performed for a transnational medical information project in Europe.[24] The Royal Canadian Mounted Police has also participated in multi-agency PIAs including multilateral information agreements regarding immigrants.[25]

A PIA framework should facilitate multi-organisational and trans-border PIAs. Of special importance here is co-operation between data protection authorities (DPAs) from jurisdictions involved and mutual recognition of decisions, if any, taken by DPAs (or any other public authority) with regard to such trans-border PIA. However, this issue requires further investigation.

---

[20] Cf. Art 18 of the 1995 Data Protection Directive; Commission nationale de l'informatique et des libertés (CNIL), *Which countries in Europe have adopted a Data Protection Officer?*, March 2012. http://www.cnil.fr/english/topics/dpo-in-europe/

[21] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 455.

[22] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook*, 2nd ed., Auckland, 2007, p. 14. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf

[23] Karol, Thomas J., *A Guide To Cross-Border Privacy Impact Assessments*, Deloitte & Touche, 2001. http://www.isaca.org/Knowledge-Center/Research/Documents/Guide-to-Cross-Border-Privacy-Impact-Assessments-2001.doc

[24] Di Iorio, C.T., F. Carinci, J. Azzopardi et al., "Privacy impact assessment in the design of transnational public health information systems: the BIRO project", *Journal of Medical Ethics*, Vol. 35, 2009, pp. 753-761.

[25] Royal Canadian Mounted Police (RCMP), *Privacy Impact Assessment Executive Summaries*. http://www.rcmp-grc.gc.ca/pia-efvp/index-eng.htm

2.1.7. Relation to prior checking

A PIA and prior checking could be complementary.

Although these two tools can be seen as complementary, there are at least two substantial differences between them. In the field of personal data protection, the first crucial dissimilarity is about their main aim, i.e. authorisation: even though there are differences in implementation of prior checking, which is foreseen by Art 20 of the 1995 Data Protection Directive,[26] data protection authorities are usually allowed to stop processing operations they deem to be non-complying with legislation before these operations start, while a PIA is rather a self-assessment tool, regardless of its compulsory nature or not. It does not prevent the start of a project, even though the assessment might be negative. Second, while prior checking is an *ex post* examination made by the authority, a PIA – conducted or commissioned by the project's proponent (data controller) itself – examines the project *ex ante*, thus having a possibility to impact the design of the project.

The best elements of these two tools should be combined. If a PIA carried out indicates that the project would present high degree of specific risks for the protection of privacy and personal data, a data protection authority should be consulted. The authority should be empowered to prohibit the deployment of the project and provide a set of recommendations to avoid or minimise such risks. This is the way in which the proposed General Data Protection Regulation links prior checking and data protection impact assessment (cf. Art 34).

2.2. The core PIA elements

2.2.1. An on-going process

A PIA should be regarded and carried out as a process and not only as a single task of completion of a report. A PIA process starts early and continues throughout the life cycle of the project.

The main objective of a PIA is to avoid or minimise negative impacts on privacy. The process of identifying, discussing and dealing with privacy and data protection issues should be on-going throughout a project and perhaps even after it has been implemented as new issues might arise that were not evident at the outset of the project's development. A PIA is a process that should start as early as possible, well before the project becomes operational and when it is possible to influence decision-making (cf. 3.2.1 below) and it should be carried out throughout the project's lifetime (cf. 3.4 below). The PIA report is a crucial element of the PIA process, but it is not its ultimate objective.

The key elements of the PIA process are the following (cf. also 3.3 below):

1. Determining whether a PIA is necessary (threshold analysis),
2. Identifying the PIA team and setting terms of reference,
3. Description of the proposed project,
4. Analysis of the information flows and other privacy impacts,
5. Consultation with stakeholders,
6. Risks management,
7. Legal compliance check,

[26] Le Grand, Gwendal and Emilie Barrau, "Prior Checking, a Forerunner to Privacy Impact Assessments", in Wright and De Hert, pp. 97-116. Charlesworth, Andrew, "Appendix H – Broad jurisdictional report for the European Union", in *Privacy Impact Assessments: International Study of their Application and Effects*, a report prepared for the Information Commissioner's Office, the UK, October, 2007. http://www.ico.gov.uk/upload/documents/library/corporate/-research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

8. Formulation of recommendations,
9. Preparation and publication of the report,
10. Implementation of recommendations,
11. External review and/or audit,
12. Revisiting PIA if the project in question changes.[27]

2.2.2. Scalability

A PIA policy should allow organisations to carry out a PIA appropriate to their own circumstances. A PIA policy should allow scalability of the PIA process.

Because organisations vary greatly in size, because the extent to which their activities intrude on privacy varies, and because their experience in dealing with privacy and data protection issues differs, it is difficult to provide for a "one size fits all" PIA policy. A PIA policy should be flexible, allowing organisations to carry out a PIA appropriate to their own circumstances (cf. 2.1.4 above).

The scale and scope of a PIA should generally be in line with the scale and scope of a project and should be commensurate with potential privacy risks identified during the threshold analysis (cf. 3.2.2 below). A more elaborate PIA – and more resources for carrying it out – will be needed for a complex project.

2.2.3. All privacy types

As the rights to privacy and to protection of personal data are fundamental rights in the European legal order, for ensuring the highest level of protection thereof, a PIA should address all types of privacy issues and not only the protection of personal data.

2.2.3.1. Privacy vs. data protection

There are number of schools discussing the scope of privacy. For example, Clarke considers four conventional yet overlapping categories: privacy of personal information, of a person, of personal behaviour and of personal communications.[28] For the PRESCIENT project, the research consortium has identified seven types of privacy: of a person, of thought and feelings, of location and space, of data and image, of behaviour and action, of communications, and of association, including group privacy.[29] Solove argued that the conceptions of privacy could be grouped in six categories: the right to be let alone, limited access to the self, secrecy, control over personal information, personhood and intimacy.[30] Rössler has analysed three dimensions of privacy: decisional privacy, informational privacy, and local privacy (i.e. privacy of the household).[31]

At the European level, the content of privacy for legal purposes can be securely derived from the pertinent case law of the European Court of Human Rights. The Court has ruled that Art 8 of the European Convention on Human Rights – with its four components of private life, family life, home and correspondence (communications) – can cover a wide range of issues such as

[27] Cf. also Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", presentation prepared for a workshop in Sopot, Poland, 25 April 2012. www.piafproject.eu
[28] Clarke, Roger, *What's 'Privacy'?*, 2006. http://www.rogerclarke.com/DV/Privacy.html
[29] Gutwirth, Serge, Michael Friedewald, David Wright, Emilio Mordini et al., "Legal, social, economic and ethical conceptualisations of privacy and data protection", Deliverable D1 of the PRESCIENT project [Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment], p. 8. http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf. See also 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, 2012, pp. 3-32.
[30] Solove, Daniel J., "Conceptualizing Privacy" *California Law Review*, Vol. 90, 2002, p. 1087.
[31] Rössler, Beate, *The Value of Privacy*, Polity Press: Cambridge, 2005, p 86.

integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, gender, health, identity (i.e. a right to have some control over identity markers such as one's name), sexual orientation, protection against environmental nuisances and so on; the list is not exhaustive. Interestingly, the Court has affirmed that it is neither possible nor necessary to determine the content of privacy in an exhaustive way.[32]

However, privacy and data protection are not entirely equivalent.[33] On the one hand, privacy is broader than data protection; the latter is a tool to protect the former. Both fundamental rights – to privacy and to data protection – participate in the protection of the political private sphere, although in different ways. Firstly, privacy sets prohibitive limits that shield the individual against the public authorities and other powers warranting a certain level of opacity of the citizen, whilst data protection channels legitimate use of power, imposing a certain level of transparency and accountability. Secondly, the content of the right to privacy is broader than data protection as it does not only deal with the processing of personal information.

On the other hand, data protection has a broader scope than privacy, as it deals with any processing of personal data, no matter whether or not such processing interferes with the privacy of an individual. Data protection provides for a number of fair information principles and empowers the data subject with certain rights, like the right to information, to access or to rectification. Furthermore, the processing of personal data can affect many more rights than simply the right to privacy, like freedom of expression, freedom to conduct a business, the right to property, including intellectual property, prohibition of discrimination, rights of the child, a high level of human health protection and the right to an effective remedy.

With regard to the proposed General Data Protection Regulation, it draws on Art 16 of the Treaty on the Functioning of the European Union (TFEU), providing for protection of personal data and as such it is aimed at data protection objectives only. Art 33 of the proposal, introducing a data protection impact assessment, could not have been based on Art 8 of the EU Charter of Fundamental Rights as the Charter does not extend the competences of the Union. In addition, DPAs in the EU deal mostly with informational privacy and not with other areas. Therefore, such a broader tool could be mandated by means other than the proposed Regulation, i.e. by soft law.[34]

---

[32] Most recently, the Court stated that in *Nada v. Switzerland*, Application no. 10593/08, Judgement of 12 September 2012 , § 151. "[The Court] reiterates that 'private life' is a broad term not susceptible to exhaustive definition (see, for example, *Glor v. Switzerland*, no. 13444/04, § 52, ECHR 2009; *Tysiąc v. Poland*, no. 5410/03, § 107, ECHR 2007-I; *Hadri-Vionnet v. Switzerland*, no. 55525/00, § 51, 14 February 2008; *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III; and *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 66, ECHR 2008). The Court has found that health, together with physical and moral integrity, falls within the realm of private life (see *Glor*, cited above, § 54, and *X and Y v. the Netherlands*, 26 March 1985, § 22, Series A no. 91; see also *Costello-Roberts v. the United Kingdom*, 25 March 1993, § 36, Series A no. 247-C). The right to private life also encompasses the right to personal development and to establish and develop relationships with other human beings and the outside world in general (see, for example, *S. and Marper*, cited above, § 66)."

[33] Serge Gutwirth and Paul De Hert have been amongst the very first to emphasise the difference between the legal rights to privacy and to data protection. Beyond the different scope and modus operandi of each legal tool, they conceptually ground the difference between the two rights with respect to their nature as constitutional tools, one being a tool of opacity (privacy), the other being a tool of transparency (data protection). Cf. further De Hert, Paul, and Serge Gutwirth, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence", Institute for Prospective Technological Studies – Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, pp. 111-162. http://ftp.jrc.es/EURdoc/eur20823en.pdf; Paul De Hert and Gutwirth, Serge, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104.

[34] With regard to terminology, cf. 2.2.3.3.

2.2.3.2. Beyond PIA

It is worth mentioning that there are some proposals to go beyond a "traditional" understanding of a PIA.

Consistent with 2.2.3.1 above, one could argue that a combination of both *privacy* and *data protection* impact assessment might be necessary. On the one hand, a PIA focuses on all privacy aspects. On the other hand, it is not clear yet whether a PIA does indeed seek to determine whether the processing operations comply with the procedural guarantees provided by data protection, what is the impact of the processing of personal data on other fundamental rights, etc. While the first impact assessment would focus on the violations of all the different aspects of the right to privacy, the second would focus also on the respect of the procedural guarantees featured by the right to data protection.

Raab and Wright have proposed to extend PIAs to assess the impact of surveillance on broader range of individual and societal values (such as dignity or autonomy) as well as on other rights and freedoms, arguing that a PIA presupposes only a perspective on some dimensions of privacy that might be affected by surveillance.[35]

Wright and Mordini, on the other hand, have anticipated a framework of an ethical impact assessment, as the development and deployment of information and communications technologies fuelled by personal data might raise not only privacy concerns, but also ethical ones. This ethical impact assessment can be integrated with a PIA or, at least, both could be conducted concurrently. However, a detailed analysis of these tools is beyond the scope of this deliverable.[36]

Finally, De Hert argues for "a larger assessment exercise, going beyond privacy and data protection" because – from a human rights perspective – it makes sense to go to a full assessment of risks and threats. Furthermore, as the nature of certain right is absolute, e.g. prohibition of torture, almost no interference is allowed.[37] He further recalls the example of the European Parliament who in its resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection explicitly asked the Commission to "carry out an impact assessment relating to *fundamental rights*" (emphasis added) and to consult the European Data Protection Supervisor, the Art 29 Working Party and the Fundamental Rights Agency.[38]

2.2.3.3. Terminology

There is some confusion with regard to terminology. Three terms – i.e. privacy impact assessment (PIA), privacy risk management (PRM) and data protection impact assessment (DPIA) – describe similar yet different tools. Despite that these three concepts have a lot in common, these terms cannot be used interchangeably.

First, "privacy impact assessment" is a term that has been used worldwide to describe the tool that is the subject matter of this deliverable. Second, the Information and Privacy Commissioner

---

[35] Raab, Charles and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in Wright and De Hert, pp. 363-383.

[36] Wright, David and Emilio Mordini, "Privacy and Ethical Impact Assessment", in Wright and De Hert, pp. 397-418.

[37] De Hert, Paul, „A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in Wright and De Hert, pp. 72-74. Cf. also European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, Brussels, 6 May 2011, SEC(2011) 567 final.

[38] European Parliament, *Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection*, Strasbourg, P6_TA(2008)0521. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0521+0+DOC+XML+V0//EN

of Ontario as well as the French data protection authority use the term "privacy risk management".[39] While the management of privacy risks is a core part of a PIA (cf. 2.2.6 below), a PIA is a part of a broader risks management approach within an organisation (cf. 3.1.1 below). Third, in the proposal for the reform of the EU data protection framework, the European Commission has used the term "data protection impact assessment" (DPIA) that describes a tool that focuses on data protection issues only.

However, for the sake of clarity and legal certainty, consistent terminology should be used. In the European context, once the proposed General Data Protection Regulation passes into law, a term "data protection impact assessment" should be used to refer to the tool described therein.

2.2.4. Accountability

An organisation should be able to demonstrate that a PIA has been carried out adequately.

Accountability-based mechanisms have been suggested as a way of encouraging data controllers to implement practical tools for effective data protection, in particular as an answer to the challenges posed by the information and communications technologies.[40] In the field of data protection, in general terms, accountability not only consists in adopting and implementing the appropriate measures (i.e. the requirement of efficiency) but also in being able to demonstrate – upon request – that such measures have been taken (i.e. the requirement of transparency).[41]

Certain organisational measures are, in the perspective of the Art 29 Working Party, essential for ensuring real effectiveness to the accountability principle. These include, among others:

- the establishment of internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc.),
- mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory thereof,
- the appointment of a data protection officer and other individuals with responsibility for data protection;
- offering adequate data protection, training and education to staff members,
- the implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc.), and
- performance of privacy impact assessments in specific circumstances.[42]

There is a striking resemblance between the above-mentioned organisational measures and the requirements for the PIA environment and infrastructure (cf. 3.1 below). Therefore, on the one hand, a PIA is a constitutive element of accountability and, on the other hand, a PIA can only be successfully conducted in a sound accountability framework. Thus said, PIAs should be

---

[39] Information and Privacy Commissioner of Ontario, *Privacy Risk Management, Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default*, April 2010. http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf; Commission Nationale de l'Informatique et des Libertés (CNIL), *Gérer les risques sur les libertés et la vie privée*, June 2012, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf (French version); Commission Nationale de l'Informatique et des Libertés (CNIL), *Methodology for Privacy Risk Management*, June 2012. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf (English version).

[40] Art. 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, Brussels, 13 July 2010, at 1. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf. De Hert, Paul, "Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law", in Guagnin, Daniel et al. (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, 2012, pp. 193 - 232.

[41] Art. 29 Working Party, *Opinion 3/2010*, at 28.

[42] Ibid., at 13 and 41.

understood as a part of a bigger accountability concept and should be presented that way to the project's sponsors.

With regard to PIAs, a PIA policy should require that an organisation – being accountable for protecting personal data in general terms – should in particular be accountable for carrying out a PIA. Specific measures with this regard include, among others, fulfilment of the transparency requirements (cf. 2.2.5 below), personal accountability of the senior officials for the quality and adequacy of a PIA (cf. 3.2.3 below), review or audit (cf. 2.2.7 below) and sanctions for non-compliance (cf. 2.1.3 above).

2.2.5. Transparency

A PIA process should enjoy at least a minimum level of transparency. Both the assessor and the stakeholders must have all relevant information to assess the privacy and data protection implications of the proposed project. This does not preclude due respect for sensitive information (cf. 2.2.5.4 below).

First, in a broad context, transparency is a requirement of democracy. A central premise of democratic government – the existence of an informed electorate – implies a free flow of information.[43] Furthermore, a decision-making process should be based on facts and needs to be fair. A true assessment can only be made when all the details are known. Elements such as the cost of technology and health implications need to be made public.[44] However, the level of transparency differs in the public and private sectors: simplifying, public authorities "owe" more information to their citizens than private entities to their customers.

Second, transparency is a building block of accountability (cf. 2.2.4 above).

Third, transparency is a building block of public confidence and trust. Transparency demonstrates that the organization treats privacy seriously, and consequently its customers or citizens. To some extent, it is a public-relations tool too.

The requirement of transparency in PIA is of a twofold nature: (1) of the process itself, and (2) about disclosure of relevant information. The latter can be split into three sub-categories: stakeholders' involvement (cf. 2.2.5.1 below), publication of the PIA report (cf. 2.2.5.2 below) and a central registry of PIAs carried out (cf. 2.2.5.3 below).

2.2.5.1. Stakeholders' involvement

Stakeholders, as representative as possible, including the public, if applicable, should be identified and informed about the planned project and of the PIA process. Their views should be sought and taken into consideration (cf. 3.3.3 below). The PIA policy should provide explicit mechanisms for stakeholders' consultation.

The key for understanding the rationale for public participation in impact assessments lies partly in the need to compensate for the deficiencies of political representation and partly in the insufficiency of scientific knowledge for proper risks management.[45]

---

[43] National Research Council, Committee on Risk Perception and Communication, *Improving risk communication*, Washington: National Academies Press, 1989.
[44] Wright, David and Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in Wright and De Hert, p. 75.
[45] For more details, cf. Wright, David, Raphaël Gellert, Serge Gutwirth and Michael Friedewald, "Minimizing technology risks with PIAs, precaution and participation", *IEEE Technology & Society*, Vol. 30, Issue 4, Winter 2011, pp. 47-54.

Political representation in so-called modern democracies is characterised by an asymmetrical exposure to risk: political decisions will first and foremost affect citizens. Therefore, citizens might eventually criticise political officials, not simply for the fact that decision-making in situations of uncertainty inherently carries an irreducible element of risk, but more particularly, for the behaviour of such officials who, because of personal interest, turpitude or negligence, happen to engage in paternalistic attitudes that resort to lenient justification or even to the concealment of risk-creating decisions that might affect large parts of the population without the latter benefiting from them whatsoever.[46] In other words, citizens have the right to be associated with decisions that carry risk for them.

The procedural principle is based upon the evidence that situations of uncertainty (i.e. potential risk) are not based upon a complete ignorance of the situation, but the incompleteness of knowledge regarding these situations. Therefore, it is crucial to take into consideration all points of view, even the views of a minority, in order to have as complete a picture of the situation as possible. The so-called risk society results partly from an ever-increasing complexity of technical and scientific knowledge that has gone beyond our control. Hence, the management of risk cannot solely be based upon scientific knowledge. However, this does not mean cutting all links with reason to be replaced by e.g. a heuristics of fear. Rather it consists in anchoring decision-making into a new rationality, based upon collective deliberation, which is better equipped than pure scientific expertise to deal with situations of uncertainty.[47]

In general, there are many good reasons why organisations should engage stakeholders in a PIA, some of which can be found in the ISO 27005:2008 standard on information security risk management. Engaging stakeholders provides a means to:

- provide assurance of the outcome of the organisation's risk management,
- collect risk information,
- share the results from the risk assessment and present the risk treatment plan,
- avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision-makers and stakeholders,
- support decision-making,
- obtain new information security knowledge,
- co-ordinate with other parties and plan responses to reduce consequences of any incident,
- give decision-makers and stakeholders a sense of responsibility about risks,
- improve awareness.[48]

Consultation with key stakeholders is basic to the PIA process. If a PIA is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. The objectives of a PIA cannot be achieved if the process is undertaken behind closed doors. In a complex project applying powerful technologies, many segments of the population are affected. It is intrinsic to the process that members of the public provide input to the assessment, and that the outcomes reflect their concerns.[49] Even if consultation does not increase support for a decision, it may clear up misunderstandings about the project and, at least, gain the respect of stakeholders.

When it comes to the PIA process, there are three main reasons for involving stakeholders. First, engaging stakeholders, including the public, if applicable, will help the assessor to discover risks and impacts that she might not otherwise have considered. Technology development is often too complex to be fully understood by a single agent. A consultation is a way to gather fresh input on

[46] Godard, Olivier, "Le principe de précaution, une nouvelle logique de l'action entre science et démocratie", *Philosophie Politique*, No. 11, May 2000, p. 21.
[47] Godard, op. cit., pp. 16-19.
[48] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 467.
[49] Ibid., p. 466.

the perceptions of the severity of each risk and on possible measures to mitigate these risks. Stakeholders may have some information, ideas, views or values that the project manager had not previously considered or might find that stakeholders place much greater weight on some issues that the organisation had regarded as relatively minor. They may be able to suggest alternative courses of actions to achieve the desired objectives and may have some good suggestions for resolving complex issues, e.g. some safeguards that would minimise the risks.[50]

Merely complying with privacy laws will provide organisations with no assurance that their schemes will be acceptable to citizens and consumers.[51] Consulting stakeholders may provide a sort of a test how the project would work and help to eliminate options that meet with significant resistance.[52] The assessor will be able to learn the public reaction to the project. By consulting stakeholders, the assessor may forestall or avoid criticism that they were not consulted. Thus, as a minimum, the assessor will gain stakeholders' understanding and respect as well as will earn some good will and trust by consulting stakeholders who might otherwise be among her chief critics.

Second, from the human rights perspective, decision-making procedures should involve the persons affected by technologies. Art 8 of the European Convention on Human Rights does not contain an explicit procedural requirement, but the decision-making process leading to measures of interference must be fair and such as to afford due respect to the interests of the individual as safeguarded by the right to privacy. This requirement of fairness implies at least that evidence is gathered and that the impact of technologies are studied in advance, that the public has access to this evidence and that individuals can come up in court against decisions that, they feel, do not take their viewpoint into consideration.[53]

Within the scope of application of the Charter of Fundamental Rights of the EU, the right to good administration (Art 41) requires "every person to be heard, before any individual measure which would affect him or her adversely is taken".

Third, stakeholders' engagement contributes to the requirement of transparency (cf. 2.2.5 above). Transparency, through a greater level of scrutiny, is critical to improving the quality of privacy analysis. Public disclosure may also provide additional assurance that privacy impacts are being appropriately considered in the development of programs, plans and policies – essentially holding each institution organisation to public account for the adequacy of the privacy analysis that was undertaken. Whereas improved public reporting can be a constructive tool for organisational development and the enhancement of internal privacy practices, poor public reporting may have a profoundly damaging effect on the trust of individuals in their government.[54]

2.2.5.2. Publication of the PIA report

The PIA report should be made public and should be easily accessible.

Having prepared the PIA report, the organisation should make it publicly available, e.g. publish it on its website (cf. 3.3.6 below). Once a PIA is revisited (cf. 3.4 below), a new version should be made equally available, with a reference to the previous one.

---

[50] Ibid., p. 468.
[51] Ibid., p. 466.
[52] Health Information and Quality Authority [Republic of Ireland], *Guidance on Privacy Impact Assessment in Health and Social Care*, December 2010, p. 18. http://www.hiqa.ie/system/files/HI_Privacy_Impact_Assessment.pdf
[53] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 469.
[54] Stoddart, Jennifer, „Auditing Privacy Impact Assessments: The Canadian Experience", in Wright and De Hert, p. 434.

2.2.5.3. Central public registry

There should be a public register of PIAs actually carried out and it should be easily accessible.

The creation of a public register of PIAs helps create a body of knowledge and examples of good practice so that assessors can learn from the experience of others. It encourages undertaking similar assessments. The registry could be also used by the public to better understand the substance of projects. Precedents for central indexes exist, such as those of environmental impact assessments. From the formal point of view, by creating a single window of access, regardless of the origin of a PIA report, such a register simplifies the search process.

These benefits could be equally achieved by the means of a single central register, created and managed by the public authorities (e.g. DPAs), or a number of interoperable registers, as long as it is not too burdensome to find and access a particular PIA report. The register should preferably have a digital form.

Following the deliberations about sensitive information (cf. 2.2.5.4 below), the register should lead, e.g. by the means of hyperlinks, to the full PIA reports, their abridged versions, or summaries thereof. It is an open issue whether a register should contain also links to documents on audit, review or any other form of the involvement of data protection authorities.

2.2.5.4. Sensitive information

State secrets and commercially sensitive information should not be made public.

Put simply, during the PIA process, the assessor needs to engage stakeholders, who are usually external to the organisation, and make public the final report, or – at least – parts or summaries thereof. These might require disclosure of information that is not meant to reach the external people or the public in general, e.g. state or trade secrets. Some organisations may be afraid to disclose such information because they fear negative publicity or they have concerns about competitors learning something they do not want them to. In particular, companies often want to avoid making public the description of data flows.[55] State security and commercially sensitive information should not be legitimate reasons for not conducting a PIA.

Therefore, with regard to the final report, an organisation could redact the document and place confidential information in an annex and publish only the main body of the report. Alternatively, an organisation might create and publish a summary of the report. (Summaries are usually better understandable by the individuals who lack technical and/or legal expertise. However, such summaries must be meaningful: it is not enough to state that risk were identified and appropriate mitigation is planned with no hint to what those might be.) Both solutions are acceptable as long as the essence of the assessment is properly documented. With regard to stakeholders, some of them might be consulted e.g. through closed discussion sessions with non-disclosure agreements.

In the case of the public sector, if a PIA report is not available in its entirety, individuals wanting to see the entire PIA could apply under the freedom of information legislation.

2.2.6. Risks management and legal compliance check

Risks management and legal compliance check are core elements of PIA. To that end, effective procedures for risk management should be identified and/or developed.

[55] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 453.

Next to the risks assessment and risks mitigation (cf. 3.3.4 below), the legal compliance check can be seen as the second crucial element of PIAs. Legal compliance check aims at ensuring the projects would not breach relevant privacy and data protection laws (legislation, jurisprudence, etc.) In particular, if a project is of a trans-border nature, the assessor should ensure it complies with relevant laws in all jurisdictions in which it would be deployed.

Risks management cannot be equalled to legal compliance check since the former is broader in scope than the latter. Risks management goes beyond merely assessing the risks of non-compliance with relevant laws and examines all possible risks to the protection of privacy and personal data. However, nothing precludes assessing compliance with laws whilst risks are being managed.

A PIA should be viewed also as part of a broader risks management practice within an organisation and should be integrated thereto, i.e. linked with other risk mitigation tools (cf. 3.1.1 below). Proper risks management methodologies should be identified and/or developed.

2.2.7. Audit and review

A PIA process should be subjected to external review and/or audit.

Independent third party review and/or audits are critical to ensure a PIA was properly carried out and its recommendations implemented. Audits and reviews are a function of the principle of accountability and lead to improvements in PIA practice. It is all too easy for project proponents to say initially that they accept and would implement suggested changes, only to find reasons later to backslide, and either partially or wholly abandon their initial commitment.[56] Furthermore, in case a DPA reviews or audits a PIA, this offers them a better understanding of PIAs and impacts their role in PIA policy (cf. 2.3 below).

A DPA will not have the resources to review all of the PIAs, but it could perhaps undertake a random review of some of them (e.g. 10 per cent). The organisation is more likely to take the time to prepare a proper PIA especially if it thinks that it might be that "one-in-10" that gets reviewed. In any case, the report should be made available to a DPA upon request. (The requirement to send all PIA reports to DPAs for their information seems too burdensome.)

2.3. Leadership of the data protection authorities

Data protection authorities (privacy commissioners) should play a key role in PIA policy and practice. In particular, they should promote PIAs and facilitate the PIA process by providing expertise, guidance and advice for policy-makers and assessors as well as – possibly – by reviewing and providing feedback of (selected) PIAs actually carried out.

The interest in PIAs is growing, particularly among the policy-makers and DPAs. Some DPAs have already been performing certain "PIA-like" activities, such as prior checking[57] or prior consultation. Some DPAs have been more active and have already issued some guidance material for PIA and some others are considering such a step. Of equal importance are awareness raising and training activities.

As PIAs vary considerably as a policy and practice, even within single jurisdictions, there is a strong need to identify common standards and good practice. This is a function of a need for

[56] Waters, Nigel, „Privacy Impact Assessment – Great Potential Not Often Realised", in Wright and De Hert, p. 154.
[57] Art 20 of the 1995 Data Protection Directive. Cf. also 2.1.7 above.

harmonisation and global standards regarding data protection (cf. 2.1.4 above).[58] This activity should result in high-quality and user-friendly guidance material (cf. 2.1.2.3 above), especially in handbooks and templates, which should be regularly updated to accommodate new developments and to address new challenges. This task is foreseen mainly for DPAs but it could be fulfilled equally by international data protection forums (e.g. the Art 29 Working Party or the Berlin Group),[59] standardisation organisations (e.g. ISO) or private sector (e.g. industry associations). In case the law requires a PIA be made on a standard template (form), a DPA is in the best position to set one.

Next, a DPA should be able to provide information (e.g. by seminars and workshops) and comments regarding the PIA policy and process for assessors. The assessor should be able to seek advice from the DPA free of charge, as there is general fear of "getting it wrong".[60] Throughout the PIA process, informal and voluntary consultations may take place.

The DPA will learn what makes an effective PIA and will be able to pass on "good practice" to all PIA assessors. These might include PIA acceptance, approval (or some other form of signing off), review and audit. The expertise of DPAs could be used to review and provide feedback on PIAs actually carried out. As DPAs might not have enough resources, they could do so selectively, i.e. evaluate a sample of PIAs each year (cf. 2.2.7 above).

A DPA should be provided with PIA report upon request. In case a PIA is connected with prior checking (cf. 2.1.7 above), a DPA might be empowered to block certain projects if the risk is too high.

[58] Art. 29 Working Party, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168, Brussels, 1 December 2009, p. 10. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[59] International Working Group on Data Protection in Telecommunications (IWGDPT). http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt

[60] Oppé, Thomas, "PIAs in the UK: the regulatory approach", keynote speech at the PIAF 2nd Workshop, Sopot, 24 April 2012. http://www.piafproject.eu

3. Recommendations for PIA practice

3.1. PIA environment and infrastructure

PIAs are only good as the process that supports them. Therefore, PIA requires – within an organisation – high-level support, embedding in a governance model, privacy expertise and a "privacy culture". Professional independence of the assessor must be ensured.

A successful PIA is only a tool. Its utility depends on how it is used and who uses it. It depends on service providers having the correct processes and resources in place to carry out a PIA. These include an internal architecture supporting privacy, awareness raising and the independence of the assessor.

3.1.1. Internal architecture

There should be some internal administrative architecture to support PIA policy objectives: support of the executive, assigned accountabilities, internal agency structure, awareness (culture, promotion and education), personnel and professional expertise, including identifying specific staff who are personally responsible for privacy.[61] A mechanism for evaluation and monitoring compliance, including monitoring of PIA recommendations (cf. 3.4 below), should be put in place. Privacy assessments only make sense when they are embedded in a governance model that supports the implementation of the results. Companies believe that this delivers tangible benefits.[62]

An organisation should create and embed administrative linkages between PIAs and other risk mitigation tools, e.g. a PIA should be part of internal risk management. Organisations can manage another area of risk – similar to those posed by technology, economic factors or the environment. However, in many organisations it is not possible for capacity reasons, or it will never be accepted by executive, to maintain separate systems of risks management.[63]

3.1.2. Privacy awareness

An organisation is responsible for ensuring that all its employees are sensitive to the privacy implications. Insinuating privacy into daily practice, on-going targeted training and raising awareness and raising the profile of PIAs within an organisation substantially contribute to the level of in-house privacy expertise and internal "privacy culture". Examples include, among others, codes of conduct, general e-learning, blogs and use of an intranet as well as privacy screen-savers and games.[64] Creating general awareness of the policy requirements respecting privacy is often the first step towards ensuring that managers fully consider the privacy impacts of their plans and priorities at the time an initiative is conceived.

3.1.3. Professional independence of the assessor

An organisation should ensure the assessor acts with professional independence. A PIA should be an honest investigation. The assessor must recognise the bias and subjectivity that she might bring to the task, declare that in the report (i.e. subjective assessments must be clearly flagged as such), seek empirical backing for any position taken (e.g. public surveys on attitudes) and present a range of scenarios with different consequences evident for decision-makers.

---

[61] Cf. further Stoddart, Jennifer, „Auditing Privacy Impact Assessments: The Canadian Experience", in Wright and De Hert, p. 423, in particular Fig. 20.1.
[62] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 447.
[63] We are grateful to Kristine Rytter for this remark.
[64] Bräutigam, Tobias, "PIA: Cornerstone of Privacy Compliance in Nokia", in Wright and De Hert, pp. 259-261.

Adequate resources (i.e. time, budget and manpower) are necessary to fulfil the requirement of the independence of the assessor (cf. 2.1.5 above). 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. Furthermore, 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 senior officials.

3.2. Preliminary issues

3.2.1. Threshold analysis

An organisation should perform a preliminary threshold analysis (initial assessment) of every project to determine whether a PIA is necessary. An assessor should be able to seek non-binding advice from a DPA in case of doubt.

There are several reasons why a PIA process may be initiated. These include:

1. a requirement in law, specifying situations in which there is an obligation to carry out a PIA,
2. appreciation by an organisation that a proposal has broad and significant implications that should be subjected to PIA, and
3. public concerns, perhaps arising from media-fanned rumours about an initiative.[65]

However, even if there is a legal requirement to carry out a PIA, the general nature of such an obligation may not always make clear when a PIA is required. In such a situation, a DPA should provide non-binding advice for the assessor (cf. 2.3 above).

For example, Wright and De Hert argue there are at least two ways one could address the question of whether a PIA is necessary. One is to ask whether the project involves the processing of personal data or could impact any type of privacy. If the answer is yes, then a PIA is necessary. A second way to address the question is to consider some brief "what if" scenarios the aim of which would be to contemplate what could go wrong if the organisation proceeds with the project. If these scenarios show there are some privacy risks, then a PIA should be initiated.[66] This is the broadest approach – yet the most difficult to implement – and the most preferable from the privacy protection point of view, as it triggers PIA simply when there might by *any* impact on privacy (i.e. *all* types thereof) by *any* project.

As the second example, Clarke argues that a PIA is applicable to a proposed project that has significant potential impacts on, or implications for, groups of people or organisations other than the primary sponsor. The need for a PIA arises from the scale of the proposal's impacts and implications, and is independent of the question as to whether it is a public or private sector initiative. Examples of schemes that are likely to require PIAs include:

- databases involving personal data, especially where:
  - the data is sensitive;
  - the number of people involved is substantial; and/or
  - the record about each person is intensive;

[65] Clarke, Roger, *Privacy Impact Assessment Guidelines*, 1998, at 2. http://www.xamax.com.au/DV/PIA.html
[66] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 462.

- identification and identity authentication schemes, especially proposals for multi-purpose identifiers, intrusive identifiers such as biometrics, and digital signature initiatives;
- schemes whose effect is to convert anonymous or pseudonymous transactions into identified transactions;
- smartcard-based schemes;
- location and tracking schemes, e.g. in mobile telephony and other forms of telecommunications;
- intelligent transportation systems; and
- law enforcement and national security information systems, and criminal intelligence systems.[67]

As the third and final example, the PIA guide of the Victoria Information and Privacy Commissioner (Australia) offers a list of 17 questions to determine if a PIA is necessary. It is advised that if the answer to one or more of their questions is yes, then a PIA should be seriously considered. Thus, it is asked in the guide if the project will involve:[68]

1. *"Establishing or amending a public register (as defined in the Information Privacy Act)?*
2. *The collection of personal information, compulsorily or otherwise?*
3. *A new use for personal information that is already held?*
4. *A new or changed system of regular disclosure of personal information, whether to another part of State or local government, or to the private sector, or to the public at large?*
5. *Restricting access by individuals to their own personal information, e.g., by affecting the Freedom of Information Act?*
6. *New or changed confidentiality provisions or secrecy provisions relating to personal information?*
7. *New or changed offences relating to the misuse of personal information?*
8. *A new or amended requirement to store, secure or retain particular personal information?*
9. *A new requirement to sight, collect or use existing ID, such as an individual's driver's licence?*
10. *The creation of a new identification system, e.g., using a number, or a biometric?*
11. *Linking or matching personal information across or within agencies?*
12. *Exchanging or transferring personal information outside Victoria?*
13. *Handling personal information for research or statistics, de-identified or otherwise?*
14. *Powers of entry, search or seizure, or other reasons to touch another individual (e.g., taking a blood sample)?*
15. *Surveillance, tracking or monitoring of individuals' movements, behaviour or communications?*
16. *Moving or altering premises which include private spaces?*
17. *Any other measures that may affect privacy?*"

If the threshold analysis results in a conclusion that a PIA is not required, this should be reasoned. On the other hand, if a PIA is required in circumstances that do not justify an assessment, then limited privacy policy or compliance resource may be expended needlessly.

---

[67] Clarke, Roger, *Privacy Impact Assessment Guidelines*, 1998, at 2. http://www.xamax.com.au/DV/PIA.html

[68] Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments – A guide for the Victorian Public Sector*, 2nd ed., Melbourne, April 2009, p. 22. http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide/$file/guideline_05_09_no1.pdf; An analysis of threshold assessments in various PIA frameworks worldwide is provided in Wright, Wadhwa, De Hert and Kloza, ch.ch. 2-8.

3.2.2. Determination of the scale and scope of PIA

The assessor should determine the appropriate scale of a PIA, commensurate with the risks identified.

A PIA should be conducted in a manner that is commensurate with the potential privacy risk identified. If, after the threshold analysis, the risks are not significant, then the scale and scope of a PIA could be limited. If the risks are significant, then a PIA should be more detailed. The size or budget for a project is not a useful indicator of its likely impact on privacy.[69]

The guidebook issued by the UK Information Commissioner's Office distinguishes between full-scale and small-scale PIAs. The phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalised and does not warrant as great an investment of time and resources in analysis and information gathering.[70] However, the distinction between a full-scale and small-scale PIA seems artificial.

3.2.3. Roles and responsibilities

Consistent with section 3.1, an organisation should determine what are the roles and responsibilities of its officers with regard to PIAs, i.e. who initiates, who carries it out and who approves them. A team of experts, including external ones, might be necessary. Depending on the complexity of the project, an organisation might need to set terms of reference for the PIA process and its plan. Continuity of the PIA process should be ensured. A senior executive officer should be held accountable for the quality and adequacy of a PIA.

Regardless of whether the PIA process results from a legal obligation or from an organisation's own decision (cf. 3.2.1 above), it is an internal issue of the organisation who should initiate and conduct a PIA. The suggestion to start a PIA could come from anyone in the organisation: it could be a senior official, a project manager or an internal data protection officer. A PIA could be conducted in-house or it could be outsourced.[71]

Consistent with the complexity of the project and the scale of a PIA (cf. 3.2.2 above), the assessor may need to form a team to accomplish the task. The privacy expertise is crucial here but it does not exclude other fields. The team could bring together expertise from information security experts, lawyers, operations managers, ethicists, public relations experts, communications professionals (if the stakeholder's involvement requires so), etc. The team might involve external experts too. As the PIA progresses, the assessor may find that she needs still other expertise.

The project manager and/or the organisation's senior management might need to decide on the terms of reference for the PIA team, its budget and its timeframe. The management board should decide how implementation of recommendations would be monitored. The assessor might need to prepare a plan for conducting a PIA.

An organisation should ensure that the PIA process is continued and completed in case it is transferred to another organisation (cf. business continuity).

---

[69] Office of the Victorian Privacy Commissioner, p. 5.
[70] Information Commissioner's Office, p. 26.
[71] There are a few reasons in favour of a project manager conducting a PIA. First and foremost, it is her accountability for the risks posed by her project. Secondly, she will be most informed about the project and should be able to detect where there are risks. Finally, doing a PIA internally would help embed privacy awareness throughout the organisation.

In order to fulfil the accountability requirement (cf. 2.2.4 above), a senior official should approve the final results of the PIA process. A senior official should "sign off" a PIA. Senior officials are unlikely to affix their signature to a sub-standard document where there is a risk that they will be criticised subsequently for having agreed to an inadequate or otherwise deficient PIA.

3.3. The PIA process

3.3.1. Early start

The PIA process (cf. 2.2.1 above) should start as early as possible so that it can influence the design of the project.

The PIA process should genuinely affect the development of the project as this is the only way its ultimate objective can be achieved: to adapt the project to the results obtained, improving it from the moment that it is conceived and preventing certain risks from occurring.[72] A PIA should start when it is possible to influence decision-making, when polices are being formulated and key choices about the project are being made, but before completing detailed design or development work,[73] and not well after the main design parameters are set, significant costs incurred or when the project starts. However, if a PIA is conducted too early, its results may be vague as there may not be enough information available about the project, the scope and proposed information flows to properly consider the privacy implications and as such the PIA may need to be revisited.[74]

3.3.2. Project description

A project subjected to a PIA should be adequately described. So should be information flows and its impact on other privacy types, if applicable.

The project description contains two elements: (1) a general description of the project, and (2) a mapping of information flows and/or an analysis of its impact on other privacy types. The description should be detailed enough to allow for a comprehensive identification and management of privacy risks. Details of the project could be added as the PIA process progresses.

3.3.2.1. General description of the project

The PIA process needs to be primed by the preparation of a conceptual design and issues paper, which should contain the following:[75]

- a description of the context or setting in which the proposal is being brought forward (including relevant social, economic and technological considerations), leading to a statement of the motivations, drivers or opportunities underlying it;
- a statement of the proposed scheme's objectives;
- the initial conceptual design of the scheme. This should reflect the primary sponsor's current thinking about the matter. It should be at a level such that participants can develop an understanding of the idea and ponder its impacts and implications; but it should not be so advanced or detailed that salient design features have been pre-determined;

[72] Wright, David and Paul De Hert, "Findings and Recommendations", in Wright and De Hert, p. 465.
[73] Office of the Information and Privacy Commissioner (OIPC) of Alberta, *Privacy Impact Assessment Requirements for Use with the Health Information Act,* Edmonton, 2009, p. 13. http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf
[74] Health Information and Quality Authority [Republic of Ireland], *Guidance on Privacy Impact Assessment in Health and Social Care*, December 2010, p. 18. http://www.hiqa.ie/system/files/HI_Privacy_Impact_Assessment.pdf
[75] Clarke, Roger, *Privacy Impact Assessment Guidelines*, 1998, at 7. http://www.xamax.com.au/DV/PIA.html

- brief descriptions of options and sub-options that the primary sponsor has identified, including both those already dismissed, and those that remain under consideration;
- an outline cost/benefit analysis;
- an outline of first-order impacts and second-order implications, as perceived by the primary sponsor at the time of publication;
- descriptions of the PIA process and of the broader scheme development process;
- lists of involved organisations, advocates, stakeholder groups and representatives who have been invited to contribute to the PIA (cf. 3.3.3 below);
- addenda, as appropriate.

It is vital to the effectiveness of a PIA that the stakeholders involved have an understanding of the technologies used in the project. This may necessitate that the assessor make available technical briefings and documentation.

Furthermore, this section should also discuss:

- who is responsible for the project,
- who is undertaking the development of the project,
- when it is expected to be deployed and/or to become available,
- who is the target of the project (e.g. the market or group),
- how the end-users might be affected by the project;
- organisational privacy management structure and policies, including
  - how senior management is involved in decision-making related to privacy,
  - how the organisation identifies, investigates and responds to privacy incidents, e.g., privacy breaches, how the organisation decides to notify affected parties and how it seeks to learn from an incident; an organisation might attach its privacy statement here;
- important milestones and, especially, when decisions are to be taken that could affect the project's design.

3.3.2.2. Information flows and other privacy implications

The content of such description is a function of the requirements of the main data protection legal instruments. Such a description should address: the creation, collection, retention, use, disclosure, transfer and erasure of personal data as well as issues such as accuracy, security, safeguards, the exercise of the data subject's rights and who is the data controller and who is the data processor.

In case a project does not deal (only) with informational privacy (personal data) but with other types of privacy (too) (cf. 2.2.3 above), this section should address (also) how the individual's privacy might be affected.

3.3.3. Stakeholders' consultation

An organisation should identify stakeholders, inform them about the project, seek their views and duly take them into consideration. The consultation process should be documented.

3.3.3.1. Identification

The assessor should identify stakeholders, i.e. those who are or might be interested in or affected by the project. The range and number of stakeholders to be consulted should be a function of the privacy risks identified (3.3.4 below) and the assumptions about the frequency and consequences of those risks and the numbers of individuals who could be impacted.

Depending on the complexity of the project, a consultation plan might be needed and communications professionals engaged.

The stakeholders might include people who are internal as well as external to the organisation. They could include public authorities, customers, civil society 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.

If the stakeholders engaged in the PIA process are not reasonably representative of those concerned about or affected by the project, there is a risk that the validity of the PIA may not be accepted. If an organisation tries to "fix" a consultation by consulting only "safe" stakeholders, i.e. those who will go along with its point of view, it actually does itself a disservice, not just by making a sham of the process, but also by not achieving the advantages and benefits of a consultation which is aimed at identifying risks, obtaining fresh information and finding solutions, in other words of achieving a "win-win" result so that everyone benefit.

The full range of stakeholders may not be immediately apparent to the assessor. Some stakeholders may only become apparent as the PIA process progresses. Stakeholders should be invited to suggest other stakeholders who are not represented in the group but should be or might wish to be.

3.3.3.2. Information

The stakeholders should receive enough information about the project, in a clear manner, in order to make an informed contribution. One of the first things to be done in engaging stakeholders is to explain to them what the process will be, why the consultation is being undertaken, how long it might last, what results are expected and how they might be used. Stakeholders' involvement and opposition to given facts and choices need to be possible not only at the beginning but also later on throughout the process, e.g. when new facts emerge. Stakeholders who are not experts, i.e. mainly the public, should be informed about the project in a clear and understandable way, e.g. by avoiding complex jargon.

3.3.3.3. Consultation

There are several different ways of consulting stakeholders and the assessor should consider which would be most appropriate in the circumstances. These include: interviews, surveys, public hearings, workshops, focus groups and on-line consultations.[76]

A timeframe for consultation should be provided. The deadline for submitting answers should be proportionate to the complexity of the project. For example, during the policy-making process in the United Kingdom and the European Union normally a minimum of 12 weeks are allowed for consultation. If the public is the main stakeholder, it might happen that they would not reply to the call and thus not provide their views at all. By providing a reasonable deadline, an organisation acts diligently.

3.3.3.4. Consideration

The views of the stakeholders, gathered as a result of consultation, should be duly taken into consideration. The assessor should take a position on each of them and should provide justification if any is rejected.

---

[76] For a list of possible techniques, see e.g. OECD, *Stakeholder Involvement Techniques*, Paris, 2004, pp. 30-32. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf

3.3.4. Risks management

The assessor should identify, assess and mitigate all possible risks and other negative privacy impacts. Residual risks should be justified.

Any risk management is only as good as the methodology underlying it. This means if the methodology is flawed, then so is the assessment.[77] The PIA risk management process described below has been adopted for RFID applications.[78] However, other methodologies exist.[79]

3.3.4.1. Risks assessment

The first step in the risk assessment phrase is to identify conditions that may threaten or compromise protection of privacy and personal data. A good project description (cf. 3.3.2 above) and proper consultation with stakeholders (cf. 3.3.3 above) contribute here. Risks could arise from vulnerabilities in the scheme under consideration (e.g. a lack of security safeguards or the fact that sensitive information is processed) as well as from external threats (e.g. theft or misuse of data). The risk assessment should take into account the impacts on both the individual and on society.

A PIA process requires a relative quantification of these risks. The assessor should consider the likelihood and consequences of privacy risks occurring. Finally, the risk assessment requires evaluating the applicable risks. Thus the assessor should consider: (1) the significance of a risk and the likelihood of its occurrence, and (2) the magnitude of the impact should the risk occur. The resulting risk level can then be classified as low, medium or high.

3.3.4.2. Risks mitigation

The second step is to identify controls, options and alternatives that can help to minimise, mitigate or eliminate the identified privacy and data protection risks. Controls are either of a technical or non-technical nature. Technical controls are incorporated into the project, e.g. access control mechanisms, authentication mechanisms and encryption methods. Non-technical controls, on the other hand, are management and operational controls, e.g. policies or operational procedures. Controls can be categorised as being preventive or detective. The former inhibit violation attempts, while the latter – warn operators about violations or attempted violations. A PIA should entail cost-benefit analyses of various mitigation strategies in order to arrive at decisions.

The identified risks and their associated risk levels should guide the decision on which of the identified controls are relevant and thus need to be implemented. An organisation might as well abandon the project (cf. 3.3.7 below).

---

[77] Shrader-Frechette, Kristin, *Risk Analysis and Scientific Method. Methodological and Ethical Problems with Evaluating Societal Hazards*, Reidel, Boston, 1985, p. 17.

[78] Cf. footnote 6.

[79] There are various risk management methodologies, such as: International Organization for Standardization (ISO), *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, Geneva, 2011; International Organization for Standardization (ISO), *Risk management – Principles and guidelines*, ISO 31000:2009, Geneva, 2009; 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, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; European Network and Information Security Agency (ENISA), *Emerging and Future Risks. Framework Introductory Manual*, Heraklion, 2010. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual/at_download/fullReport. For the purposes of managing privacy and data protection risks, cf. methodologies mentioned in footnote 39.

Following the PIA, one or more risks may remain if a new project is to be undertaken. However, the benefits may be such that these risks are regarded as worth taking. If the organisation has decided to proceed with the project despite it raising some privacy risks, the assessor should provide justification for the intrusions upon privacy.

The PIA report (cf. 3.3.6 below) should include a section that identifies the options and alternatives available to the organisation in order to mitigate, avoid, transfer, eliminate or accept the privacy risks identified by the PIA. The report should say why particular options or alternatives were rejected or discounted and why a particular course of action has been recommended.

3.3.5. Legal compliance check

The assessor should ensure that the project complies with any legislative or other regulatory requirements.

The assessor should identify applicable laws, regulations, standards and jurisprudence. Non-binding instruments, such as the opinions of the Art 29 Working Group, should be taken into account too.

3.3.6. Recommendations and report

An assessor should provide recommendations and an action plan for their implementation. A PIA should be concluded by the final report, which is a "living instrument", updated if necessary (cf. 3.4 below).

The assessor should conclude her work with a set of detailed recommendations with an action plan, setting also the timeline for their implementation. The assessor should be clear to whom her recommendations are directed – towards different units within the organisation, the project manager, the CEO, employees or employee representatives (e.g. trade unions) or third-party applications developers.

A PIA process should result in a report. The report has a value as a "corporate memory". Unless its format is mandatory (cf. 2.3 above),[80] following the PIA process described in the present deliverable, the report should contain at least:

1. introduction and background information (cf. 3.1 and 3.2 above), including who undertook the PIA, her contact details and where to find further information and other sources of help and advice;
2. a description of the project, of the information flows and of the impacts on privacy;
3. results of the consultation of stakeholders;
4. a description of the risk assessment and risk mitigation phases, including the alternatives considered;
5. analysis of legal compliance;
6. recommendations;
7. annexes, if necessary.

Aberration from any of the requirements of the PIA process, if any, should be reasoned in the report.

A report should be made available to a DPA upon request. With due respect for sensitive information, the report or its summary should be made public (cf. 2.2.5.2 above).

[80] An example of a template for a PIA report is offered by the Office of the Victorian Privacy Commissioner (Australia). http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessment-report-template/$file/guideline_05_09_no3.doc

3.3.7. Decision and implementation of recommendations

An organisation should take a position on each of the recommendations, i.e. whether it will implement them or not and why.

Following the PIA report, an organisation should take a position on its recommendations. It does not need to accept all of them, but it should say which ones they have implemented already or intend to implement and which they do not intend to and the reasons why. Some recommendations might be implemented even during the drafting phase of the PIA report.

If the project is too intrusive upon privacy, the organisation may decide to cancel the project altogether.

3.3.8. Audit and review

The final PIA report should be audited or reviewed externally.

The final PIA report, documenting the whole PIA process, should be subjected to an external audit or review (cf. 2.2.7 above).

3.4. PIA is a living instrument

The implementation of the recommendations should be monitored. A PIA should be revisited each time a project is changed and such a change impacts privacy.

Many projects undergo changes before completion. The need to revisit and update a PIA when a project changes and this change has privacy implications is a function of regarding PIA as a process (cf. 2.2.1 above). Depending on the magnitude of the changes, the assessor might need to revisit the PIA as if it were a new initiative. However, if the changes are of minor importance the assessor might conclude that a revisit of a PIA is not necessary.

4. Bibliography

This section lists academic papers prepared so far by the consortium throughout the lifetime of the PIAF project.

Books

Wright, David, and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Chapters in books

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, 2012, pp. 3-32.

Wadhwa, Kush, and David Wright, "eHealth - Frameworks for Assessing Ethical Impacts" in Carlisle George, Diane Whitehouse and Penny Duquenoy (eds.), *eHealth: Legal, Ethical and Governance Challenges*, Springer-Verlag, Berlin, 2012.

Articles in peer-reviewed journals

Friedewald, Michael, David Wright, Serge Gutwirth and Emilio Mordini, "Privacy, data protection and emerging sciences and technologies: towards a common framework", *Innovation: The European Journal of Social Science Research*, Vol. 23, No. 1, March 2010, pp. 63-69. http://www.informaworld.com/smpp/content~content=a922417231~db=all~jumptype=rss

Gellert, Raphaël, and Dariusz Kloza, "Can privacy impact assessment mitigate civil liability? A precautionary approach", in Erich Schweighofer et al. (eds.), *Transformation juristischer Sprachen. Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012*, Österreichische Computer Gesellschaft, Wien, 2012, pp. 497 – 505.

van Lieshout, Marc, Michael Friedewald and David Wright, "Reconciling privacy and security", *Innovation: the European Journal of Social Science Research*, Vol. 25, No. 3-4, October 2012 [forthcoming].

Wadhwa, Kush, "Privacy Impact Assessment Reports: A Report Card", *info*, Vol. 14 Issue 3, 2012. http://www.emeraldinsight.com/journals.htm?issn=1463-6697&volume=14&issue=3

Wright, David, "Should privacy impact assessment be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131. http://cacm.acm.org/magazines/2011/8

Wright, David, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, Vol. 13, No. 3, September 2011, pp. 199-226. http://www.springerlink.com/content/nw5v71087x60/

Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol. 28, No. 1, February 2012, pp. 54-61. http://www.sciencedirect.com/science/journal/02673649

Wright, David, Raphaël Gellert, Serge Gutwirth and Michael Friedewald, "Minimizing technology risks with PIAs, precaution and participation", *IEEE Technology & Society*, Vol. 30, Issue 4, Winter 2011, pp. 47-54.

Deliverables

Wright, David, Kush Wadhwa, Paul De Hert, and Dariusz Kloza (eds.), *PIAF*: *A Privacy Impact Assessment Framework for data protection and privacy rights*. Deliverable D1. Prepared for the European Commission Directorate General Justice. 21 September 2011. www.piafproject.eu

Hosein, Gus, and Simon Davies. *Empirical research of contextual factors affecting the introduction of PIA frameworks in the Member States of the European Union*. PIAF Deliverable D2, August 2012. www.piafproject.eu

Other publications

Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", Presentation prepared for a workshop in Sopot, Poland, 25 April 2012. www.piafproject.eu

Wright, David, and Kush Wadhwa, "A template for preparing a privacy impact assessment report", Presentation prepared for a workshop in Sopot, Poland, 25 April 2012. www.piafproject.eu