D1.2.4

Cloud Computing –
Data Protection Impact Assessment

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	1st October, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D1.2.4/ 1.0
Activity and Work package contributing to the deliverable:	Activity 1 / WP 1.2
Due date:	September 2013 – M36
Actual submission date:	7th October 2013

Responsible organization:	ULD
Editor:	Ninja Marnau
Dissemination level:	Public
Revision:	1.1 (without confidential Annex)

Abstract:	This deliverable includes a proposed methodology for a Data Protection Impact Assessment in the TClouds context.
Keywords:	Data Protection, Privacy Enhancing Technologies, Privacy Impact Assessment, Data Protection Impact Assessment, Data Protection Goals, Unlinkability, Transparency, Intervenability, Confidentiality, Integrity, Availability

Editor

Ninja Marnau (ULD)

Contributors

Ninja Marnau (ULD)

Meiko Jensen (ULD)

Eva Schlehahn (ULD)

Ricardo Morte Ferrer (ULD)

For Version 1.1: Marit Hansen (ULD)

Disclaimer

This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose.

The user thereof uses the information at its sole risk and liability. The opinions expressed in this deliverable are those of the authors. They do not necessarily represent the views of all TClouds partners.

Executive Summary

In this deliverable we assess the data protection and data security impact of the benchmark use cases and infrastructure components developed within the last three years of the TClouds project.

As the concept a Data Protection Impact Assessment is still fairly vague, we first collect, analyze and compare existing Privacy Impact and Data Protection Impact Schemes. Based on those lessons learned we propose a more comprehensive and less sector-specific assessment scheme based on six Data Protection Goals.

In the full version of this deliverable, a Data Protection Impact Assessment according to that scheme is performed with respect to TClouds use cases and infrastructure components. This part is left out in the public version due to confidentiality restrictions defined in the Document of Work of the TClouds project.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 TClouds – Trustworthy Clouds

TClouds aims to develop trustworthy Internet-scale cloud services, providing computing, network, and storage resources over the Internet. Existing cloud computing services are today generally not trusted for running critical infrastructure, which may range from business-critical tasks of large companies to mission-critical tasks for the society as a whole. The latter includes water, electricity, fuel, and food supply chains. TClouds focuses on power grids and electricity management and on patient-centric health-care systems as its main applications.

The TClouds project identifies and addresses legal implications and business opportunities of using infrastructure clouds, assesses security, privacy, and resilience aspects of cloud computing and contributes to building a regulatory framework enabling resilient and privacy-enhanced cloud infrastructure.

The main body of work in TClouds defines an architecture and prototype systems for securing infrastructure clouds, by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and by assessing the resilience, privacy, and security extensions of existing clouds.

Furthermore, TClouds provides resilient middleware for adaptive security using a cloud-of-clouds, which is not dependent on any single cloud provider. This feature of the TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on a cloud-of-clouds.

1.2 Activity 1 – Legal and Business Foundations for Cross-Border Computing

The Scope of Activity 1 is to identify requirements and boundaries for cloud computing. The Activity aims at providing a guidance framework to address both legal requirements and business interests in cross-border infrastructure clouds.

Based on the expertise and input from users and stakeholders, the activity researches relevant interests, drivers and obstacles for the use of cloud computing services for privacy-sensitive and business-critical applications – with a focus on the implication of cross-border cloud deployment.

Furthermore, an analysis of the European legal framework for data protection and data security will identify the regulatory foundation for cloud computing and lead to an investigation of its privacy impact.

The Activity addresses the business impact of cloud computing as well as the accompanying privacy and security concerns. Requirements derived from this tense relationship of business benefit and regulatory boundaries will be mapped to organizational, contractual and technical measures and enablers.

1.3 Work Package 1.2 – Legal Implications and Impact of Cross-Border Cloud Implementations

The objective of WP1.2 is to provide and define legal requirements for cloud computing in cross-border scenarios. Different legislation und jurisdiction on privacy- and IT-related issues of cloud computing will be analyzed. The analysis will enable us to provide solutions and additional measures for cross-border cloud scenarios. Furthermore, the privacy impact of cross-border clouds using well-known and standardized methods will be analyzed.

1.4 Deliverable 1.2.4 Cloud Computing – Data Protection Impact Assessment

1.4.1 Structure

In this deliverable we assess the data protection and data security impact of the benchmark use cases and infrastructure components developed within the last three years of the TClouds project.

We start by collecting and analyzing existing Privacy Impact and Data Protection Impact Schemes and describe benefits and shortcomings. Based on those lessons learned we propose a more comprehensive and less sector-specific assessment scheme based on six Data Protection Goals.

1.4.2 Deviation from Work Plan

We decided to name the deliverable Data Protection Impact Assessment instead of Privacy Impact Assessment to emphasize the more European scope and also honor the introduction of the Data Protection Impact Assessment to the proposed Data Protection Regulation for the EU.

1.4.3 Relation to Other Deliverables

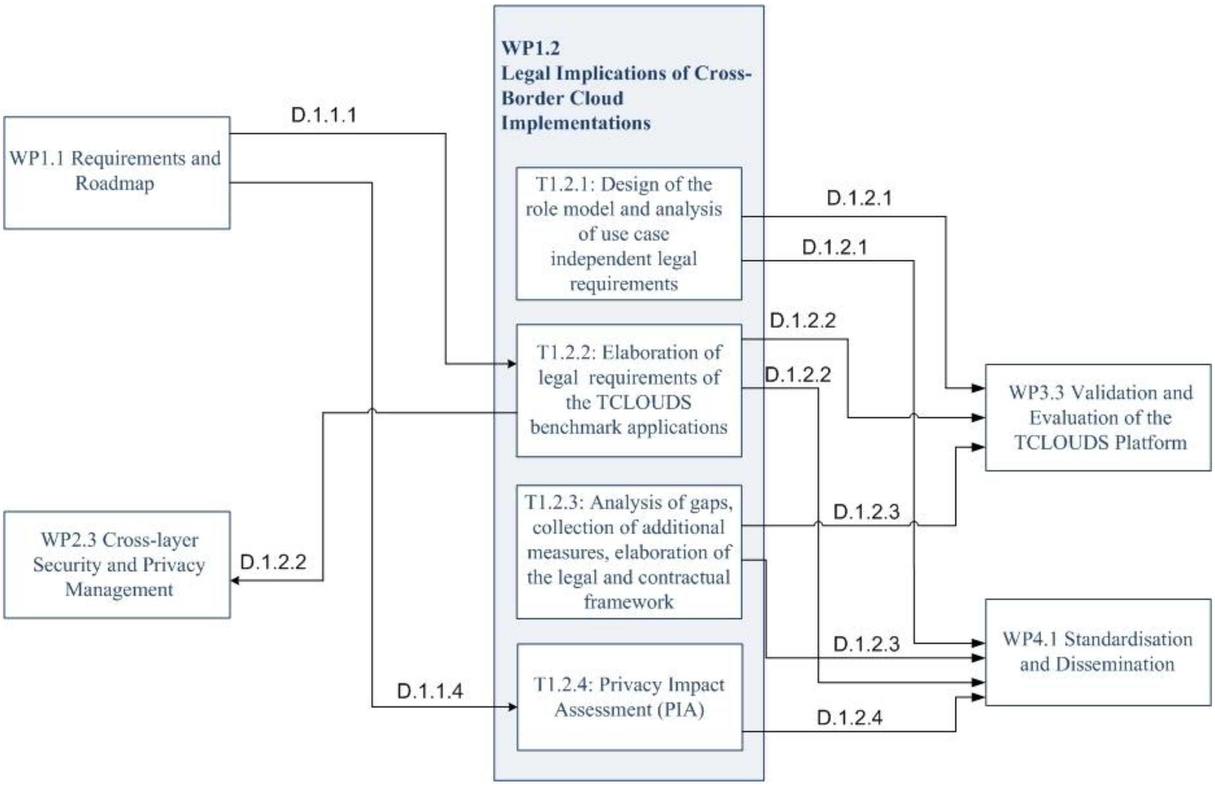
WP1.2
Legal Implications of Cross-Border Cloud Implementations
WP1.1 Requirements and Roadmap
D.1.1.1
T1.2.1: Design of the role model and analysis of use case independent legal requirements
D.1.2.1
D.1.2.1
T1.2.2: Elaboration of legal requirements of the TCLOUDS benchmark applications
D.1.2.2
D.1.2.2
WP3.3 Validation and Evaluation of the TCLOUDS Platform
T1.2.3: Analysis of gaps, collection of additional measures, elaboration of the legal and contractual framework
D.1.2.3
WP2.3 Cross-layer Security and Privacy Management
D.1.2.2
D.1.2.3
WP4.1 Standardisation and Dissemination
D.1.1.4
T1.2.4: Privacy Impact Assessment (PIA)
D.1.2.4

Figure 1: WP1.2 Interdependencies

Chapter 2

Introduction to Privacy Impact Assessment and Data Protection Impact Assessment

A **Privacy Impact Assessment** (PIA) in the most general definition is a process whereby a conscious and systematic effort is made to assess the privacy and data protection impacts of a specific project, process or application with the view of taking appropriate actions to prevent or at least minimize those impacts.

The concept of PIA has been known since the mid-1990s and has become more popular in recent years. There exist varying definitions:

- "A process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and examined" (Clarke, 1999)[1]
- "A privacy impact assessment is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts"[2]
- "A privacy impact assessment (PIA) is a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize the negative impacts"[3]

Similar to the lack of a common (legal) definition, there is no common methodology for the assessment. In recent years several institutions published guidelines and frameworks to conduct a PIA. These will be described and analyzed in Chapter 2. The problem of these frameworks is that they are mostly restricted to a specific application, industry sector or national law. As of today, no universal framework or methodology could prevail.

In this document we try to develop a universal approach that is methodically clear and easy to apply to any project or application, allowing comparability and usefulness in all member states of the EU.

Under the EU Data Protection Directive 95/46/EC there was no mandatory PIA for data controllers on European level. This could change within the next years as the European Commission officially introduced a "**Data Protection Impact Assessment**" (DPIA) in the 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

[1] Roger Clarke: *Privacy impact assessments*. Xamax Consultancy Pty Ltd., Version of 19 April 1999, with small revisions subsequently, and progressive enhancements to the Bibliography, most recently 26 May 2003, http://www.rogerclarke.com/DV/PIA.html.

[2] David Wright, Paul de Hert: *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

[3] PIAF EU Project, Final Deliverable http://www.piafproject.eu/ref/PIAF_D3_final.pdf

data published in January 2012 (hereafter: Regulation). Article 33 explicitly states requirements for a Data Protection Impact Assessment and when it becomes mandatory (see below). To address these future legal requirements we will stick with the term Data Protection Impact Assessment (DPIA) in this document.

Article 33 Data protection impact assessment

1. *Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*
2. *The following processing operations in particular present specific risks referred to in paragraph 1:*

   (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

   (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

   (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;

   (d) personal data in large scale filing systems on children, genetic data or biometric data;

   (e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
3. *The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.*
4. *The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.*
5. *Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.*
6. *The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.*
7. *The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*

Chapter 3

Related International Concepts for PIA

The first guidelines and frameworks about PIA were released after 1998, and at this time different specialists and consultants were working on this concept and its development in Australia, Canada, Hong Kong, New Zealand and USA The UK Information Commissioner's Office published a PIA Handbook in 2007 and revised it in 2009[4]. The Madrid Resolution[5] includes the concept of privacy impact assessment in paragraph f) of section 22:

22. Proactive measures

States should encourage, through their domestic law, the implementation by those involved in any stage of the processing of measures to promote better compliance with applicable laws on the protection of privacy with regard to the processing of personal data. Such measures could include, among others […]

f) The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any method of processing personal data or substantial modifications in existing processing.

After so many years, one would expect that, given the time elapsed since the emergence of the concept; PIA had become an essential part of the rules and structures of privacy and data protection in Europe. But it is not so, we will try to expose the possible causes that have led to this situation as well as possible ways to accelerate the development and implementation of the PIA as a key figure in the field of data protection at European level.

As we mentioned before, PIA is still under construction in the EU, but recently there has been some activity in its development. The main steps were:

1. The endorsement of the European Union's (EU) Radio-Frequency Identification (RFID) PIA Framework by the Art. 29 Working Party in February 2011[6].
2. The development of a data protection impact assessment (DPIA) framework for smart metering systems[7].
3. The proposal for the new General Data Protection Regulation, released on 25 January 2012[8] which in its Art. 33 explicitly provides for a DPIA.

[4] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/ privacy_impact_assessment.aspx

[5] http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/ common/2009_Madrid/estandares_resolucion_madrid_en.pdf

[6] 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] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Between the reasons causing the short coming development of PIA in Europe, maybe the biggest one is that politicians are afraid that it could be seen as a new bureaucratic burden, the main complain coming from big companies when they face a new regulation.

Some measures which could help accelerating the development of PIA could be:

- PIAs should become mandatory. Currently PIAs are mandatory, in a kind of “indirect way” in Canada; it means government institutions are obliged to carry out a PIA and to include the results of their PIAs when they make submissions for funding to the treasury Board Secretariat. PIAs are also mandatory for US Government Agencies under the E-Government Act of 2002.In Europe, the European Commission’s Recommendation indicates that all RFID operators should assess the impact of their operations on privacy and data protection when they introduce a new system or make significant changes in the RFID application. Significant changes are those that expand the application beyond its original purposes or lead to new types of information processed; uses of the information that weaken the controls employed
- Trying to reach a better harmonization in how to conduct a PIA or a DPIA, keeping some flexibility degree in order to be able to adopt possible changes for specific sectors. Currently we have many different frameworks, guidelines and handbooks for PIAs, but sometimes they follow very different criteria they are made for a specific technology or business field (e.g. Oetzel / Spiekermann for RFID[9]), and they are not usable for another field or use.

Another aspect to consider would be who should be responsible for conducting the PIA. It is essential that the person or entity dealing thereof has a high degree of independence from the entity that commissioned the work. Possible examples include the DPO of the entity in question or an external consultant who can demonstrate unequivocally that independence.

As in other procedures related to risk assessment, a PIA should be an evolving process. It would make little sense to draw up a PIA in a timely phase of a project without having to undertake a further control of the evolution of this project.

The last deliverable of the PIAF project remarks the following points as the key elements for a PIA process:

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,
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.

[9] https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html

We will expose the main points of some different PIA frameworks, guidelines and handbook, compare them in a table and then we will try to explain which could be the main points or criteria for a better framework or guidelines.

3.1 The New Federated Privacy Impact Assessment (F-PIA)[10]

3.1.1 *Federated Identity Management (FIM)*

Along with the user, FIM architecture typically contains (a minimum of) the following roles:

- Service Provider (SP) or Relying Party (RP): A web application that provides a service to the user, but which has outsourced user authentications. This service thus “relies” on a third party to provide identity information. There will be multiple Service Providers within the FIM “ecosystem”.
- Identity Provider (IP): A website or service with which the user has established his/her identity. The IP provides identity verification service to the Service Provider, and may also be a central store of user information, to be distributed on a least-means access basis. There may be one or more IP’s in the FIM ecosystem.
- Discovery Service: A means of finding an Identity Provider that is acceptable to both the User and the Service Provider; this could be as simple as a drop-down menu on the SP’s website.

3.1.2 *What are the Goals of an F-PIA?*

1. To provide an opportunity for members to discuss, develop and codify a Federation’s privacy policies.
2. To demonstrate that privacy policies, as defined be the members of the Federation, will be met.
3. To demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.
4. An F-PIA should benefit all parties who complete, use and rely on an F-PIA.

3.1.3 *Information Lifecycle*

1. Appropriate Notice – Is the individual whose personal information is being transferred aware of the transfer?
2. Appropriate Specification – Are the federated parties appropriately aware of the limitations related to the collection, use, sharing and retention of information?
3. Appropriate Consent – Can transfers of personal information be appropriately linked to a user’s consent or choice?
4. Appropriate Control – Does the user have appropriate control over the transfer of his or her personal information?

[10] http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

5. Data minimization – Do federation members collect the minimum amount of personal information necessary?
6. Least Means Access – Do federation members transfer and access only the personal information needed to complete a particular transaction?
7. Compliance, Audit and Oversight – Is there an oversight body, or auditing or compliance mechanism, to ensure that privacy policies are met?
8. Reporting – Is there sufficient documentation of policies and procedures to help demonstrate compliance?

3.1.4 Operational Principles

1. Structure/Role Assignment – Are the roles of all federation members clearly understood and transparency defined? Do federation members know their responsibilities and obligations?
2. User understanding – Are the names or types of members of the federation, and their roles made clear for the user?
3. Identity Management at the Ecosystem Level – Do service providers have the capacity to link a user's profiles across services, in the absence of user authorization? This may be the case if a service provider serves a dual role as the identity provider. (This topic goes to the ability of federated identity formats to enable appropriate sharing limitations.)
4. User Involvement – How does the federation project against account linking, traffic and analysis? How does the federation encourage user involvement in defining controls?
5. Worst Case Scenario – Has a "disaster" scenario been considered, including steps to be taken to notify users and minimize any damage that may have resulted.

3.1.5 Implementation

The following framework might be followed when developing detailed questions in this area:

1. Awareness – Are federation members aware of the need to information and network security, and the steps they can take to enhance security?
2. Accountability – Are federation members accountable to information security, to the extent appropriate to their role?
3. Response – Is there a response action plan in place, so that federation members can co-operatively prevent, detect, and respond to security incidents?
4. Ethics – Do participants understand that their own action or inaction may harm other federation members?
5. Risk Assessment – Have all federation members individually, and at the level of federation, completed risk assessment and minimization processes?
6. Security Design and Implementation – Is security designed as an essential element of the information systems?
7. Security Management – Does the federation have a comprehensive approach to security management?

8. Reassessment/Learning – Does the federation, and federation members, have a schedule for reassessing security measures, and making modifications as appropriate, including reassessment after incidents or operational failures?

In addition to inter-federation security measures, technical questions regarding common security threats at the user federation member transaction level must be addressed. These threats may involve denial of service, message replay, spoofing, brute force, or many other common forms of online attack. Sample questions that a federation, and each of its individual members, may wish to ask include:

1. Are user interactions (beyond the log-in process itself) authenticated? If not, what alternative measure is used to prevent session hijacking?
2. Will session tokens be used? If so, what measures are in place to prevent message replay?
3. Have authentication measures been evaluated to assure that they are appropriate to the nature and sensitivity of the information?

3.2 A Foundational Framework for a Privacy by Design PIA[11]

3.2.1 Purpose of this Framework

With its focus on respect for the individual, and a user-centric approach, the Framework is intended to guide organizations towards achieving a positive-sum outcome, a win-win solution for both their customers and their businesses, by ensuring the protection of an individual's privacy without sacrificing functionality or security. Whenever the Privacy by Design (PbD) principles are applied, the result is a more meaningful understanding of privacy across the organization.

This Framework does not replace or negate the need for organizations to ensure that their privacy practices and controls meet local legislative and/or regulatory requirements. While the Framework incorporates Fair Information Principles (FIPs) as the minimum basis for privacy analysis, organizations must customize the Framework to include both local legal and environmental privacy considerations. By adopting this approach, organizations will have a single tool that captures the full spectrum of privacy issues that should be addressed in the development of the Applications.

The following were taken into account in developing the Framework:

- There is a need for both privacy and business professionals to consider privacy in a holistic manner;
- PbD, which embraces and extends the FIPs, is an approach that enables organizations to achieve this goal;
- Legislative compliance is a necessary, but not a sufficient, condition to ensure appropriate privacy protection;
- The Framework should be supplemented by industry-specific questions, jurisdictionally-specific legislative requirements, as well as considerations related to the environment in which the organization operates;

[11] http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf

- Privacy professionals should consider using this framework to augment PIA based on a compliance/regulatory approach; and
- The Framework should also provide a useful baseline for anyone concerned about delivering privacy protective Applications following the PbD Principles.

3.2.2 *Scope of the Framework*

The scope of the Framework is broader than other PIAs that focus primarily on an organization's compliance with legislative and regulatory requirements and FIPs. PbD assumes a holistic approach to privacy by transforming how an organization manages the privacy of individuals from policy and compliance to an organization-wide business issue and/or strategy. PbD adopts a holistic approach to privacy by:

- Ensuring privacy protection is embedded into information technology, business processes, physical spaces and networked infrastructures from the outset; and
- Encouraging organizations to adopt the PbD Principles into all aspects of their operations wherever and whenever PI is collected, used, disclosed, retained, transferred, and/or disposed.

The Framework discusses the application of the seven PbD Principles in three areas:

1. Information technology;
2. Accountable business processes, and
3. Physical design and networked infrastructure.

The Framework does not include discussion on local privacy drivers. As such, the Framework does not address the privacy legislation and regulatory requirements to which an organization is subject. It does require organizations to consider the political, industry, or technical environments in which the Application will operate, as well as the privacy expectations of the organization's clients and other stakeholders. However, these elements, as well as legal requirements, should be specifically tailored to the organization's unique circumstances and incorporated, where appropriate, into the Framework provided for each of the PbD Principles.

The seven PbD principles:

1. Proactive not Reactive – Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive Sum, not Zero-Sum
5. End to End Security – Full Cycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it Individual and User-Centric

Context:

- Description of the business purpose(s) of the Application;

- Discussion and analysis of the organization's current privacy and security policies, procedures and processes, as well as governance and accountability structures;
- End to end description and analysis of business processes and data flows relating to the Application, including a description of the actors involved in the collection, use, disclosure, transfer, retention, and destruction of PI;
- Detailed Analysis of the Application's privacy controls (such as those for consent management, access control and audit logging/alerting/reporting, user notification);
- Detailed description and analysis of the design of the Application, including the security features or controls; and
- Identification of privacy and security risks associated with the Application, accompanied by proposed recommendations to mitigate, or eliminate, the risks.

3.3 PIA ICO Handbook V2

The ICO[12] says the privacy impact assessment should begin as soon as possible, when the PIA can genuinely affect the development of a project. The ICO uses the term "project" throughout its handbook, but clarifies that it could also refer to a system, database, program, etc. The ICO proposes a privacy impact assessment as a process that aims to:

- identify a project's privacy impacts,
- understand and benefit from the perspective of all stakeholders,
- understand the acceptability of the project and how people might be affected by it,
- identify and assess less privacy-invasive alternatives,
- identify ways of avoiding or mitigating negative impacts on privacy,
- document and publish the outcomes of the process.

3.3.1 Initial Assessment

The PIA process starts off with an initial assessment, which examines the project at an early stage, identifies stakeholders and makes an initial assessment of privacy risks. The ICO Handbook includes an appendix with screening questions the answers to which will help the organization decide whether a PIA is required, and if so, whether a full-scale or small-scale is necessary.

3.3.2 The Five Phases of a Full-Scale PIA

3.3.2.1 Preliminary Phase

In this phase, the organization proposing the project prepares a background paper for discussion with stakeholders, which describes the project's objectives, scope and business rationale, the project's design, an initial assessment of the potential privacy issues and risks, the options for dealing with them and a list of the stakeholders to be invited to contribute to the PIA.

[12] http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/

3.3.2.2 Preparation Phase

In this phase, the organization should prepare a stakeholder analysis, develop a consultation plan and establish a PIA consultative group (PCG), comprising representatives of stakeholders.

3.3.2.3 Consultation and Analysis Phase

This phase involves consultations with stakeholders, risk analysis, identification of problems and the search for solutions. Effective consultation depends on all stakeholders being well-informed about the project, having the opportunity to convey their views and concerns, and developing confidence that their views are reflected in the outcomes of the PIA process.

3.3.2.4 Documentation Phase

This phase documents the PIA process and outcomes in a PIA report, which should contain:

- a description of the project,
- an analysis of the privacy issues arising from it,
- the business case justifying privacy intrusion and its implications,
- a discussion of alternatives considered and the rationale for the decisions made,
- a description of the design features adopted to reduce and avoid privacy intrusion and the implications of these features,
- an analysis of the public acceptability of the scheme and its applications.

3.3.2.5 Review and Audit Phase

This phase involves a review of how well the mitigation and avoidance measures were implemented.

3.4 ISO[13]

3.4.1 Privacy Impact Assessment

According to ISO, a PIA is the overall process of privacy risk identification, privacy impact analysis and privacy impact evaluation. As an input to the privacy impact assessment, the organization shall provide a proper system description.

3.4.2 System Description

The organization shall provide to the privacy impact assessment team detailed documentation on the system requirements, the system design and the operational plans and procedures. If available at this step, the security concept should also be taken into consideration.

[13] Document with restricted access.

The system requirement documentation shall contain at least:

- the purpose the system is going to be, or was designed for;
- a description of the business process that is, or will be, supported by the system.
- the list of functional requirements defined for the system and their level of obligation or implementation;
- the advanced security objectives if considered;
- if the system or its data are intended to get shared with third parties, information about with whom the system or data will be shared and for which purposes; and
- a statement on the justification for processing the PII involved in this system.

The system design documentation shall contain at least:

- an overview of the functional (or logical) architecture;
- an overview of the physical architecture;
- the structure of system databases, tables and fields;
- a data flow diagram; and
- a list of interfaces, defining the parties connected and the data fields transferred.

The operational plans and procedures documentation shall contain at least:

- the identity and user management concept for the system;
- the operational concept, especially if the system or parts of it are operated on site, externally hosted or housed, or if they are cloud sourced and in which geographical area;
- the support concept, especially listing third parties by name that are involved in supporting the system and to which degree they will have access to PII;
- the logging concept and the respective retention plans;
- the backup and recovery plans;
- the data retention and deletion plans; and
- the decommissioning concept.

3.4.3 Privacy Risk Identification

The aim of this step is to generate a comprehensive list of privacy risks based on those events that might prevent, degrade or delay the achievement of the privacy safeguarding requirements. It is also important to identify the privacy risks associated with not pursuing an opportunity of treatment. Comprehensive identification is critical, because a privacy risk that is not identified at this stage will not be included in further analysis. Identification should include privacy risks whether or not the source of those risks is under control of the organization.

3.4.4 Privacy Impact Analysis

Privacy risk analysis provides an input to privacy risk evaluation and to decisions on whether privacy risks need to be treated and on the most appropriate privacy risk treatment strategies and methods.

Privacy risk is analyzed by determining consequences and their likelihood, and other attributes of the privacy risk. An event can have multiple consequences and can affect multiple objectives. Existing privacy safeguarding requirements and IS controls and their effectiveness should be taken into account.

ISO uses a four categories scale scheme for:

- the impact of a privacy breach, using 1 for “low impact”, 2 for “medium impact” and 4 for “very high impact”; and
- the likelihood for the privacy risk to happen, using 1 for “very unlikely”, 2 for “unlikely”, 3 for “likely” and 4 for “very likely”.

3.4.5 Privacy Impact Evaluation

Privacy impact evaluation involves comparing the level of privacy risk found during the analysis process with privacy risk criteria established when the context was considered. If the level of privacy risk exceeds the privacy risk criteria, the privacy risk should be treated.

In some circumstances, the privacy impact evaluation can lead to a decision to undertake further analysis. The privacy impact evaluation can also lead to a decision not to treat the privacy risk in any way other than maintaining existing privacy safeguarding requirements. This decision will be influenced by the organization’s risk appetite or risk attitude and the privacy risk criteria that have been established.

3.4.6 Privacy Risk Treatment

Privacy risk treatment involves a cyclical process of assessing a privacy risk treatment; deciding whether residual privacy risk levels are tolerable or not; if not tolerable generating a new privacy risk treatment; and assessing the effect of that treatment until the residual risk reached complies with the organization’s privacy risk criteria. Privacy risk treatment options can include the following:

- avoidance (e.g., avoiding the privacy risk by deciding not to start or continue with the activity that gives rise to the privacy risk);
- removing the source of the privacy risk;
- transfer (e.g., transferring the risk to another party or parties (e.g., by obtaining insurance));
- mitigation (e.g., changing the nature and magnitude of likelihood or changing the consequences); and/or
- acceptance (i.e., retaining the privacy risk by choice).

3.4.6.1 Selection of Privacy Risk Treatment Options

Selecting the most appropriate privacy risk treatment option involves balancing the costs and efforts of implementation against the organizations liability for safeguarding the privacy of any PII stakeholder whose PII is controlled or processed by the organization.

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where privacy risk treatment options can impact on risk elsewhere in the organization, these areas should be involved in the decision. Though equally effective, some risk treatments may be more acceptable to stakeholders than others.

Privacy risk treatment itself can introduce privacy risks. A significant privacy risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the privacy safeguarding plan to give assurance that the measures remain effective.

3.4.6.2 Preparing and Implementing Privacy Safeguarding Plans

The information provided in safeguarding plans should include:

- what privacy principles are safeguarded against which risks;
- performance measures and constraints;
- persons who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- reporting and monitoring requirements;
- resource requirements; and
- timing and schedule.

3.4.7 Recording the Privacy Impact Assessment and Treatment Process

Risk management activities should be traceable. In the risk management process, records provide the foundations for improvement in methods and tools as well as the overall process.

Decisions concerning the creation of records should take into account:

- benefits of re-using information for management purposes;
- costs and efforts involved in creating and maintaining records;
- legal, regulatory, and operational needs for records;
- method of access, ease of retrievability and storage media;
- retention period; and
- sensitivity of information.

At the end of each privacy impact assessment, the results of each step of the privacy impact assessment and treatment process shall be recorded into a comprehensive report, containing at least:

- the system description provided
- the list of privacy risks identified;
- the privacy impact analysis output
- the privacy safeguarding plan, including the acceptance statement by the risk owners for implementing the respective privacy risk treatment; and
- a list of residual privacy risks detected during the assessment and having no treatment option assigned yet.

This report shall be filed by the person responsible for conducting the privacy impact assessment and shall formally be signed off by the organization's management responsible for the program that is controlling the processing of PII.

3.4.8 Monitoring and Review

The organization's monitoring and review processes should encompass all aspects of the privacy impact assessment and treatment process for the purposes of:

- analyzing and learning lessons from events, changes and trends;
- detecting changes in the external and internal context including changes to the privacy risk itself which can require revision of privacy safeguarding requirements and priorities;
- ensuring that the privacy safeguarding and treatment measures are effective in both design and operation; and
- identifying emerging privacy risks

3.5 Personal Health Information Protection Act (PHIPA) PIA[14]

3.5.1 Purpose of the Privacy Impact Assessment (PIA) Guidelines

These PIA Guidelines were developed as a self-assessment tool to assist health information custodians in reviewing the impact that a proposed information system, technology or program may have on the privacy of an individual's personal Health information under PHIPA.

3.5.2 Methodology for Conducting a PIA

These PIA Guidelines provide an annotated questionnaire for health information custodians that are subject to PHIPA. The questionnaire requests information of two general types: that related to the health information custodian's organizational privacy management practices (10 questions) and that related specifically to the information system, technology or program (20 questions).

These PIA Guidelines require a health information custodian to provide detailed information on the following topics:

- Organizational privacy management, including privacy policies, privacy controls and the privacy structure and organization at the health information custodian that is the major proponent of the proposed or existing information system, technology or program;
- Project privacy management, including a detailed description of:
    - The personal health information with which the proposed or existing information system, technology or program deals;
    - The sources from which this personal health information is to be obtained;
    - The circumstances in which personal health information collection is to take place;
    - The processing of personal health information;
    - The intended uses of the personal health information held or thus produced;
    - The proposed recipients and their intended use of the personal health information;

[14] http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf

- The circumstances in which personal health information processing, use and disclose are to take place;
- The safeguards which will be implemented to protect against unauthorized access, use, disclosure, modification or loss; and
- Any arrangements for audit and enforcement.

3.6 Privacy Impact Assessment in Health and Social Care[15]

3.6.1 PIA Threshold Assessment

A threshold assessment is a brief, initial assessment of a project, to determine whether its potential privacy impact necessitates a PIA. A threshold assessment should be routinely undertaken for every health information project initiated by a service provider. This applies not only to new projects but also to proposals to amend existing information systems, sources or processes.

The threshold assessment consists of a checklist of eleven questions. The questions focus on the scope of the project and the manner in which personal health information will be used.

The questions seek to ascertain, for example, whether the information will be shared or whether the project involves linking or matching of information.

Having completed the threshold assessment there are two possible outcomes for the project team. If the answer to one or more of the questions is “yes” then it is necessary to proceed with the PIA. If the answer to all of the questions is “no” it will not be necessary to complete the PIA process. In either case the completed threshold assessment should be signed and approved by the project lead and senior management and kept on the project file. For example, a threshold assessment for a major national project should be approved by the chief executive officer (CEO) of the Health Service Executive (HSE), an assessment for a new hospital patient administration system (PAS) should be approved by the CEO of the hospital and an assessment for a new general practice management system should be approved by the general Practitioner (GP) or the practice manager.

3.6.2 Identification of Risks

3.6.2.1 Stage 2 Overview

If it is deemed necessary to continue with the PIA following the threshold assessment, the process proceeds to Stage 2. Stage 2 involves identifying potential privacy risks through defining how the organization manages privacy and exploring the project’s scope, information flows and security arrangements. If risks are identified at this stage it will be necessary to proceed to Stage 3 – addressing the risks.

Stage 2 of the PIA requires the service provider to document and explore the following:

- privacy management
- a description of the project
- the project type and stage of development
- the scope of the project
- the information flows

Each of these issues is discussed in turn below.

[15] http://www.hiqa.ie/publications/guidance-privacy-impact-assessment-health-and-social-care

3.6.2.2 Privacy Management

This section relates to how the service provider manages the privacy of personal health within the organization. It is not specific to the project undergoing the PIA process but raises issues that must be addressed by any service provider processing personal health information. It explores information governance issues such as data protection and confidentiality, and staff awareness of the policies that are in place. It also examines issues around education and training of staff, and accountability for the handling of personal information, which are key information governance management issues. As this section relates to the service provider generally, and not to any specific project, it is likely that it will only need to be completed for the service provider's first PIA, although it will need to be reviewed and updated regularly.

This can significantly reduce the time input required to complete subsequent PIAs providing that the privacy management documentation is kept up-to-date.

3.6.2.3 A Description of the Project

This section requires the project team to provide an introduction and background to the project including the reasons for undertaking the project. It serves to put the project and any potential privacy risks in context. The project description should address the following:

- details of the service provider or individual proposing the project;
- the overall aims of the project (including how it ties in with the service provider's functions or activities);
- the drivers for or reasons behind the project;
- the scope or extent of the project (whether it is national, regional or local);
- any links with existing projects or programmes.

3.6.2.4 The Project Type and the Stage of Development

The project type and the stage of development should be documented. Documenting the type of project may lead a service user to the conclusion that a PIA is only necessary on one particular aspect of the project. Further, if the project is incremental it may raise issues around the existing system that need to be addressed.

It is important also to consider and document the current stage of the project. For example, if a project is at a conceptual stage all of the information that is necessary to complete the PIA may not yet be available. This may mean that the PIA may need to be revisited as the project develops and decisions are made. If completing a PIA at the conceptual stage, the team may not yet precisely know what the information flows will be or to whom it will be necessary to disclose the information. Any questions that cannot be answered will need to be revisited as the project develops in order to ensure that all potential privacy risks that may arise are fully addressed.

If the proposed project involves modifications to an existing system, the project team should first describe the existing system and then the proposed changes. Any detail of prior PIAs undertaken in relation to the existing system should also be included. If a PIA was not undertaken, it may be appropriate to consider whether one should be undertaken now.

3.6.2.5 The Scope of the Project

It is important to explore the scope of the project to determine how far-reaching its impact is likely to be. Exploring the scope of the project examines the extent to which a project involves the collection, use or disclosure of personal information. This section looks at indicators such as the proportion of the population upon which the project impacts and the effects the project is likely to have on the individuals involved. This can be the general population in respect of a national project or the population of service users of a particular service provider that may be affected by the project. Generally, the greater the scope of the project, the more detailed the PIA is likely to be.

3.6.2.6 Information Flows

This section is designed to assist in producing a clear picture of the project's information flows and in doing so draw out some possible areas where privacy risks may arise. This section essentially maps the flow of information from the time it is collected, through its use and disclosure if appropriate. It raises questions around how the personal health information will be handled and used, the purpose for its collection, methods of disclosure and safeguards in place to protect privacy.

3.6.3 Next Steps

Having completed Stage 2 of the PIA, the next steps to be taken will depend on whether or not the service provider has identified any actual or potential privacy risks.

If no privacy risks have been identified, a copy of the Stage 2 assessment should be signed by the project team and approved by senior management as appropriate. For example, for a major national project, approval of the chief executive officer (CEO) of the Health Service Executive (HSE) is required, for a new hospital patient administration system (PAS), approval of the CEO of the hospital is required and for a new general practice management system, approval of the general Practitioner (GP) or the practice manager is required. A copy should be kept on the project file and made available upon request.

If privacy risks have been identified at Stage 2, the next stage of the PIA, Stage 3, involves a full assessment of the areas that present risks and an analysis of how best to mitigate or avoid them. In some cases it may be necessary to balance the risks to privacy of personal information against the public good while having regard to legal requirements in this area.

This will require an in-depth analysis of certain aspects of the project and consultation with stakeholders who will be affected, which may include service users the general public.

3.6.4 Addressing the Risks

Risks to privacy can arise in many circumstances and in relation to many different types of health information projects involving the collection, use or disclosure of personal health information. The purpose of this stage of the PIA process is to analyze and address the types of privacy risks to individuals' personal health information identified at Stage 2. Once the risks have been identified as part of Stage 2 of the PIA process, the risks can be combined or grouped as appropriate. For example, if more than one risk with regard to sharing personal health information is highlighted, these can be grouped, analyzed and addressed together.

Stage 3 of the PIA process should be reviewed and approved by a member of senior management.

3.6.4.1 Analyze the Risks

Risk analysis is about developing an understanding of the risk. It has been defined as a systematic process to understand the nature of and to deduce the level of risk. In analyzing the risks it is necessary to determine the consequences and the likelihood of a particular event occurring, thereby determining the level of risk. Analyzing risks is not a once off exercise – it is part of a process that should be repeated whenever there is a change in the circumstances that affect a risk(12). In the case of health information projects service providers must consider the consequences of the event occurring, both to service users and to the service and also the probability of it occurring. This will enable service providers to rate the risk accordingly.

Sample questions for consideration as part of this stage include:

- If the event were to occur, what is the likely impact on the service user?
- If the event were to occur, what is the likely impact on the service provider?
- What is the likelihood of the event occurring?

Service providers should follow the processes outlined in their risk management policies for this section of the PIA. One approach to analyzing risks is through the use of a risk matrix, a useful tool for ranking and displaying risks by defining ranges for consequences and likelihood.

3.6.4.2 Address the Risks

Following the analysis of each risk (highlighted in Stage 2 of the PIA process) the next step is to identify ways to reduce or eliminate the possibility of each risk occurring.

The positive impacts of risk elimination should always be balanced against how the goals of the project will be affected. Selecting the most appropriate option involves balancing the costs of implementing this option against the benefits derived from it. In each case, the cost of mitigating a risk should be appropriate and proportionate to the value gained in terms of protection of personal health information gains.

The cost of risk mitigation at the planning stage of a project is very likely to be considerably less than the possible costs that could be incurred should changes be required to a project following implementation.

3.6.5 The PIA Report

The final output of a PIA is a report which details the proposed project, the steps that were undertaken as part of the PIA process and any subsequent recommendations. It should therefore contain the outputs of stages 1, 2 and 3 of the PIA process. A completed PIA report highlights and addresses all privacy risks associated with the project and the steps that have been taken to mitigate or avoid them. The publication of PIA reports builds a culture of accountability and transparency and inspires public confidence in the service provider’s handling of personal health information.

There are a number of benefits to preparing and publishing a PIA report, primarily to the service provider compiling it but which also extend further. These include:

- showing accountability in demonstrating that the PIA process was performed appropriately
- enabling the experience gained and lessons learned throughout the process to be shared
- both within and outside of the service provider’s organization
- empowering service users to inform themselves of the way their information is being used
- and the safeguards that are being put in place to protect it
- demonstrating to the public that their privacy has been given due consideration, thereby
- improving public trust and confidence in the service provider.

The structure and format of the report will vary depending on the project and its particular specifications. However, the report must at a minimum convey the following:

- a detailed description of the project including the objectives and justification for the project
- an overview of the PIA process undertaken explaining the outcome at each of the stages
- a copy of the threshold assessment form
- an overview of Stage 2 of the PIA process, with an emphasis on the scope and information flows of the project
- a description of the specific risks that have been identified
- a discussion of alternatives considered to mitigate or avoid these risks and a rationale for the decisions made
- a description of the privacy design features adopted to safeguard privacy
- details of any consultation that took place with stakeholders, service users or the general public
- an outline of any remaining risks that could not be resolved and a business case justifying why it has been decided to accept these risks and proceed with the project and the likely implications for the public or service users involved.

3.7 BSI RFID PIA[16] (Privacy risk assessment methodology)

3.7.1 Characterisation of the Application

Operators can use the RFID application description (see Table below, as recommended in the EC PIA Framework 2011) from the initial analysis as a starting point for the characterisation of the application.

From there, operators should complete an application characterisation that includes a detailed description of scenarios and use cases, systems and system components, interfaces, data flows and involved parties. The characterisation should clearly identify the scope, boundaries and assets (resources and information) that need to be protected.

3.7.2 Definition of Privacy Targets

The purpose of the risk analysis is to understand what is at risk. What is the privacy protection target? The PIA Framework specifies EU legislation as the starting point for risk analysis because any company's prime goal in evaluating privacy risks is to ensure legal compliance.

Framed legally, the European Data Protection Directive formulates nine privacy targets (P1 to P9):

1. Safeguard of quality of personal data
2. Legitimacy of processing personal data
3. Legitimacy of processing sensitive personal data
4. Compliance with the data subject's right to be informed

[16] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.pdf?__blob=publicationFile

5. Compliance with the data subject's right to access, correct and erase data
6. Compliance with the data subject's right to object
7. Safeguard of confidentiality and security of processing
8. Compliance with notification requirements
9. Compliance with data retention requirements

These privacy targets correspond to sections I to IX of the EU Privacy Directive 95/46/EC from 1995. And their concretions are taken directly from the EU Directive's legal articles.

3.7.3 Evaluation of Degree of Protection Demand for each Privacy Target

Even though all privacy targets are equally important for the regulator, they might have different degrees of urgency from a company perspective. For this reason, it is advisable to assess the level of privacy protection most feasible for an organization.

In security assessments, security targets (i.e. confidentiality of data) are often ranked according to the loss or damage that would result from their potential breach. Generally, the ranking of security and privacy targets is important, because companies need to be aware of their most important system weaknesses and prioritise security investments in those areas.

The degree of protection should be consistent with the negative consequences of a potential privacy breach. Such consequences can be anticipated for RFID operators and their customers (the "data subjects"). Customers can lose social standing, money or even personal freedom as a result of a privacy breach.

The leading question is "What would happen if..?" Two perspectives should be considered: the perspective of the operator and the perspective of the data subject. The resulting judgements are combined, generating an overall score that assigns each privacy target to the "low-1", "medium-2" or "high-3" protection demand category.

3.7.4 Identification of Threats for each Privacy Target

After privacy targets have been identified, they can be used to systematically deduce threats. The core question is how a privacy target is threatened. For example, compliance with ensuring transparency may be threatened by incomplete or insufficient information describing the service, or by information describing the service that is not current. The Annex III of the PIA Framework contains a relatively extensive but incomplete list of potential threats with RFID-specific examples.

In addition to application-related threats, RFID operators should also be aware of their reporting duties if the process personal data in the context of their RFID application. According to the PIA Framework, the PIA report shall be made available to the competent authorities at least six weeks before deployment. In most cases, a company's data protection official or the department responsible for the RFID deployment will prepare the PIA report for the authorities.

Additional notification requirements are specified in Section IX of the EU Data Protection Directive; if RFID operators process personal data, they must consider these requirements.

3.7.5 Identification and Recommendation of Controls Suited to Protect against Threats

The crucial step in the privacy risk assessment process is to identify controls that can help to "minimise, mitigate or eliminate the identified privacy risks" (PIA Framework). First, controls are considered that are implemented already or available for implementation. Identifying these controls helps operators to judge real threats and their likelihood. Then, operators can use the identified threats and their associated likelihood to determine which of the identified controls are relevant and must be implemented.

3.7.6 Assessment and Documentation of Residual Risks

In this step, the list of recommended controls that results form step 5 are evaluated. Recommended controls can be evaluated in terms of feasibility and effectiveness or by using a cost-benefit analysis. After the controls are evaluated, they can be sorted into a prioritised list. The result is a control implementation plan, from which residual risks are derived. Residual risks remain, for example, if an implemented control reduces the magnitude of the impact of a threat but does not eliminate the threat completely for technical or business reasons.

At this point, it should be noted that the aim of the PIA Framework has been to encourage “Privacy by Design” (PbD) and thus the implementation of technical controls wherever feasible (EC2009). As the EU Recommendation on the implementation of privacy and data protection principles in applications supported by RFID states: “… privacy and information security features should be built into RFID applications before their widespread use (principles of “security and privacy-by-design”)” (EC2009), p. 3). Consequently, the PIA Framework states as one of its explicit benefits that it fosters “privacy by design efforts at the early stages of the specification or development process” (EC2011, p. 3).

One reason that the PIA Framework and the EU Recommendation target Privacy by Design through technical controls as an explicit goal is that EU privacy regulation implies considerable information duties for companies with regards to their customers. If companies want to process personal data, they need to get the consent of their customers. To remain legally compliant, companies need to intensively communicate with their customers about privacy issues. This communication is not desirable from a company’s marketing perspective, nor is it appealing for customers, who incur considerable transaction cost. Privacy by Design therefore aims to minimize the creation of personal data in the first place through pre-emptive measures such as data minimization, anonymization of profiles and deletion rules. Companies that implement pre-emptive PbD measures consequently have much fewer reporting duties and can offer their customers a more seamless and less information-intensive service experience.

PbD also supports the need to ensure access control to and accountability for personal data. Here, authentication and authorization controls as well as logging measures are vital. Such processes enforce a certain protection level and create transparency around personal data processing.

3.8 Comparison to the Current Spanish Regulation

Currently the European Union is working on a new Data Protection Regulation, with which contains the implementation of an obligatory Privacy Data Protection Impact Assessment, DPIA for any treatment of personal data. It seems suitable to carry out a comparison between the current regulation in a European country and the raised one in the proposal of European Regulation. For this comparison we have chosen the Spanish Regulation, the Royal Decree 1720/2007.

In the current Spanish Regulation there is an obligation to register the files/filing system which any professional or organization will work with in his activity (Title V, Arts. 55-64). All files containing personal data must be registered at the Agencia Española de Protección de Datos (Spanish Data Protection Authority). If there is more than a data controller, each one must register his files.

The inscription of files supposes a work of previous control, that to a some extent can could be considered to be equivalent to a first steps of a DPIA, since it supposes requires the evaluation valuing of what types of information are going to be treated, if the processing of data will be outsourced, and it must bear in mind the rights of the affected data subjects, evaluating which kind of data will be processed and which security level must apply and establishing a procedure for the data subjects willing to exercise their rights of access, rectification, cancellation and opposition/disagreement according to the Spanish Legislation(Title III Arts. 23-36).

The Data Controller must, according to Art. 88, elaborate a Security Document (Documento de Seguridad) containing all technical and organizational measures required in the legislation. This Security Document could be only one for the whole organization or several different documents for every file and/or data process (Art. 88).

The Security Document must contain, at least, the following points:

a. The document's scope of applicability, specifying the protected resources.

b. Measures, norms, acting procedures and standards aimed to guarantee the security level established in the Regulation.

c. Roles and duties of the employees working in processes affecting personal data included in the registered files.

d. Structure of the files containing personal data and description of the information systems processing these data.

e. Procedure for notification, management and response for data breaches.

f. Procedures for backup and data recovery for automatic files and processes.

g. Special measures for transporting documents and/or storage mediums, and also for their destruction, or, if possible, for reusing the storage mediums.

If according to regulation the security level is middle or higher, the Security Document should also contain:

a. The identification of the security responsible person or persons, it is possible that an organization has more than one.

b. The periodical controls to be conducted in order to verify the fulfilment of the procedures and norms included in the document itself.

If the organization works as a data processor with data outsourced from a data controller, the Security Document will inform about which kind of data are processed and will also include a copy of the contract with the data controller.

If all the data processes affecting a file take place in the data processor's IT systems, the data controller must include this information in his Security Document. If the data processor assumes the whole data processing, it would be possible that he also assumes the responsibility for the Security Document. In those cases where the personal data of a filing or processing system are included and processed exclusively in the systems of the data processor, the data controller shall include this in the security document. When this affects the whole filing or processing systems of the data controller, he can delegate the security document to the data processor.

The Security Document must be kept updated, and it should be checked always if there are significant changes affecting the information systems, the processing systems or its organization, the information included in the files or processes. Any change affecting the security measures included in the legislation is considered as significant.

The Spanish Legislation distinguishes three different security levels: basic, middle and high, being the basic level the fall back category. In the following points we explain the criteria for each security level. (Title VIII, Arts.79-114).

a) The basic level is applicable to any process working with personal data:

At this level, the data controller will apply the needed necessary measures to inform the employees about their roles and responsibilities affecting personal data. These roles and responsibilities must be included in the Security Document. The data controller must establish a procedure for notification, management and response for data breaches affecting personal data. He will also have a registry recording which kind of breach happened, when it happened or when it was detected, who makes the notification and who receives it, which effects the data breach caused and which measures were taken to correct the breach.

The data controller must organize a control system, in order to achieve safeguarding that the system users can only access to the data needed necessary for their role. He must keep an updated registry keeping all information about users and user profiles, and also the authorized access rights for each one of them. Only employees registered as authorized in the Security Document will be able to change the foreseen access conditions. If someone from outside the organization could be able to access personal data he must be subject to the same rules as the organization's employees.

Documents and support mediums management:. When documents or support tools containing personal data (including via e-mail) are taken out of the data controller/data processor premises, an authorization from the security responsible (if there is one, because at this security level this is not compulsory, if there is no security responsible, the data controller will be responsible for this authorization) will be needed, or this authorization must be included in the Security Document.

Identification and authentication,: the data controller will adopt the necessary measures for the correct identification and authentication of the users The data controller/data processor will establish a procedure permitting a personal and unequivocal identification of any user trying to access to the IT system, and also verifying that he is an authorized user.

If the authentication procedure uses passwords, the allocation, distribution and storage procedure must guarantee confidentiality and integrity.

The Security Document will gather the regularity, never more than a year, for password changes. The passwords will be kept in an unintelligible form.

Backup and recovery: the data controller will set, and at least, a weekly system backup, as well as a recovery procedure that will guarantee that in case of a data breach he will be able to take the system back to the situation before the breach. The data controller must establish monthly revisions of these procedures.

b) Mid-level measures must be implemented, in addition to the basic-level security measures, to the following files or data treatments:

- Those including data about administrative or criminal infractions.
- Those including data for capital solvency and credit information services.
- Those whose data controller is the tax administration.
- Those whose data controllers are financial institutions for purposes related to the provision of financial services.
- Those whose data controllers social security institutions.

- Those including data about personal aspects that could allow evaluating certain aspects of the personality or behaviour of the data subject.

In the middle security level, the data controller will need to name a security responsible, or more than one if needed, and this appointment must be included in the Security Document, this appointment does not mean that the data controller/data processor is not responsible any more.

Beginning at this level, the information system will be audited at least every two years. This audit maybe internal or external and must be made available for the Data Protection Authority. The audit report will include all possible shortcomings, as well as the measures to correct them. The audit report will inform about all facts, data and observations in which it is based.

After any significant changes in the information system that could affect the legislation legal compliance, the data controller/data processor will need an extraordinary audit. After this extraordinary audit a new two years period will begin.

The audit report will include all possible shortcomings, as well as the measures to correct them. The audit report will inform about all facts, data and observations in which it is based. The audit report will be always available for the Data Protection Authority.

Documents and support mediums management: The data controller/data processor will establish a reception registry system for incoming documents and support mediums that will allow knowing which kind of document or support medium tool was received, and when it was sent, the sender’s identity, how many documents were sent, which kind of information they included, how they were sent and who was responsible for the reception (information about his authorization should be included too).

There will be also a system as described above for the outgoing documents and support mediums.

Identification and authentication: The data controller/data processor will establish a system that limits the possibility of trying reiterated the access not authorized to the system of information. That limits unauthorized access attempts to the information system.

Only authorized employees registered in the Security Document will have access to the premises containing the Information System hardware.

The data breach registry will also include the data recovery procedure, who was responsible for this procedure and which data were recovered. The recovery procedure needs the authorization of the security responsible.

c) High-level measures must be implemented, in addition to the basic-and middle level security measures, to the following files or data treatments:

- That relate to data of ideology, trade union membership, religion, beliefs, racial origin, health or sex life.
- Which contain or relate to data collected for law enforcement purposes without the consent of the persons concerned.
- Those that contain data derived from the acts of gender-based violence.

At the high level, added to all the mentioned above, the data controller/data processor will use labels for the documents and support tools management. These labels must allow an easier identification for authorized users and make this identification difficult for non-authorized users. For the distribution data support tools, the data controller/data processor will use encryption or, if this is not possible, an alternative procedure. Encryption must also be used with mobile hardware, if this is not possible, this situation must be included in the Security Document and the data controller/data processor will use alternative procedures in order to minimize the risks.

Backup and recovery: a backup and recovery procedure copy will be kept in a different place from the one where information system hardware is. This place must comply with all the security requirements included in the Regulation.

Access registry: this registry will keep, at least, the user identity, date and time of the try and if it was authorized granted or denied. If the access was granted, the registry will keep the information about the accessed file or register. The minimal period of conservation retention of these data will be two years. The security responsible will check this information monthly, and he must write a report of these reviews including the detected problems. The access registry will not be necessary if the data controller is a natural person and it is possible to guarantee that he is the only one having access to personal data. This situation must be included in the Security Document.

At this level, transmitting personal data on public or Wi-Fi networks will require the use of encryption.

Conclusion

According to our DPIA methodology we can say that the Spanish Regulation:

- follows the Policy B, its main target is to achieve compliance with the data protection legislation;
- establishes a scale of protection levels according to the data subject point of view at the moment of the compulsory registration of files – before the beginning of the activity;
- not only takes care of possible attackers outside of the organization, but also from inside and even the organization itself;
- establishes the elaboration of a document – the Security Document – as a basis for the DPIA report, which should be regularly reviewed in order to be adapted to important changes in the data processes.

The Security Document is always available for the DPA, and not having this document or having it elaborated in a wrong way would be punishable. Because it is a serious offense to keep the files premises, programs or equipment containing personal data without appropriate security measures (Art.44.3.h) Data Protection Act 15/1999) and it would be punished with fines between 40.001 and 300.000 euros

Beginning by the middle security level, organizations must be audited every two years or at any time after significant changes in the processes affecting personal data.

But we can also check the Spanish Regulation from another point of view. Robin Wright answers the question about what makes a good PIA, with the following points:

- A good PIA should be more than a compliance check.
- A good PIA should be a process.
- A good PIA should be reviewed.

According to these three points, the Spanish Regulation would give us a good PIA.

Because it is more than a mere compliance check, it is a process (prior checking, decide the applicable security levels and the necessary security measures and elaborate the security document) and it must be reviewed after every significant changes and, beginning at the middle level, audited every two years.

Paul de Hert has criticized data protection impact assessment as merely a compliance check "simply checking the legal requirements spelled out in the European Data Protection Framework". Currently there is an intensive debate about PIA, with many scholars pointing out that Privacy is more than Data Protection. The Spanish Regulation is about protección de datos / data protection, but it is important to remember what this really means: the fundamental right to informational self-determination. For this reason the compliance check should be the main target of any PIA.

As a conclusion, we can say that the Spanish Regulation gives the same, or even better, results as a PIA could give us. Maybe the right way to improve Data Protection would be to work on a better compliance with the current legislation, probably also by strengthening the position of the DPAs, because making PIA mandatory does not help if the DPAs are not able to review the PIA reports.

3.9 Conclusions for Our Own Methodology

One of the current problems for the implementation of PIAs as a valid and recognized instrument in the data protection field is the lack of a standard model that may be applicable to different business models and different application technologies.

Here we propose some criteria that could help to establish a methodology applicable to a broad spectrum of applications, projects and business models:

1. Expose clearly the purpose of the PIA in question. As long as there is no legal obligation to conduct a PIA a possible way to do this could be applying the following criteria[17]:

   - Policy A, in this case could be said that the organization is only performing a PIA in order to be able to show the report, maybe for marketing purposes, without a clear catalogue of control points and criteria to be applied. In this case, the PIA would be normally commissioned by the organization that developed the project or product to be evaluated
   - Policy B, here the purpose is to conduct intensive monitoring of the project in question, especially considering the degree of compliance with data protection regulations, and taking into account the point of view of the affected data subjects. This kind of PIA is likely to be commissioned by an organization that will use the product or process evaluated.
   - Policy C, following this approach would mean attempt to obtain a scientific evaluation of the process evaluated, trying to take into account anything that could pose a risk, and assessing potential risks or even social conflicts.

[17] Kirsten Bock, Martin Rost: *Impact Assessment im Lichte des Standard-Datenschutzmodells*, in: Datenschutz und Datensicherheit (DuD), 36(10):472-477, 2012.

2. Present clearly the risks in terms of data protection, following a control based on the 6 data protection goals and presenting a catalogue of measures to address the risks encountered. It is important to remember that all risks should be presented, checking the whole data protection field: technical and legal. “The specific data protection goals are transparency – as a prerequisite for governance and regulation of technical-organizational processes as well as for weighings related to the purpose of data processing, necessity, data thriftiness, information needs of the data subjects and so on – unlinkability – as an operationalisation of purpose bindingness/purpose separation – and the ability to intervene – intervenability – to operationalise especially data subject rights and the ability of information processing entities respective operators of systems to demonstrate verifiable that they actually have steering control over their systems and are not dominated by the system”[18,19]. These three data protection goals, together with the classic ones from data security, confidentiality, integrity, and availability, are backed by safeguarding measures.
3. Establish a scale of protection levels, taking particularly into account the data subject’s point of view. Many PIA frameworks refer to stakeholders’ consultation, but we mean something more: not only talking with them, but trying to protect them as data subjects.
4. Propose use cases in order to evaluate the real consequences that could origin the controlled application.
5. Study of the potential attackers’ perspective. For the data subject the organization itself may be an attacker, or other organizations which have access to his data (in our health use case e.g. Health Insurance companies).
6. Elaborating a PIA report explaining the whole PIA process and including recommendations to improve data protection, and planning the next steps of the PIA process.
7. As long as there is no legal obligation to make the PIA report public, it would be a good measure to inform the DPA about it and to make it available for this authority.
8. Review and audit, maybe it would be a good idea to regulate that at least organizations working with sensitive data need to be audited every two years (as it happens in Spain).

In the added table we compare the different according to these criteria.

[18] https://www.european-privacy-seal.eu/results/articles/BockRost-PbD-DPG-en.pdf

[19] https://www.datenschutzzentrum.de/guetesiegel/ Privacy_Protection_Goals_in_privacy_and_data_protection_evaluations_V05_20120713.pdf

3.10 Comparison Tables

1 Overview of International PIA Frameworks

Overview	**IPC Federated PIA**	**PbD PIA F Framework**	**ICO Handbook V2**	**ISO**	**IPC PHIPA**	**PIA Health and Social Care**	**BSI RFID PIA**
Issuer/Year	IPC (Canada) 2009	IPC (Ontario, Canada) 2011	ICO(UK) 2009	ISO 2012	IPC (Ontario, Canada) 2005	Health Information and Quality Authority (Ireland) 2010	BSI (Germany) 2012
Character	Framework	Framework	Handbook	Framework/Draft	Guideline	Guideline	Guideline
Target Audience	Federated Identity Management Services	Organizations processing Personal Information (PI)	Organizations handling personal data	Organizations processing personal identifiable information (PII)	Health Information Custodians (1)	Health and Social Care	RFID operators(EU)
Questionnaire/ Checklist	✅	✅	✅	N/A	✅	✅	N/A
Number of Questions	24	115	104 (2)	N/A	30	11(3)	N/A
Questions Publicly Available	✅	✅	✅	N/A	✅	✅	N/A
Intended Type of Answers	Yes/No+notes	Yes/No+notes	*Yes/No+notes*	N/A	*Yes/No/In Progress/N/A* + *Notes*	Yes/NO	N/A
Answers Verifiable	N/A	N/A	☑	N/A	☑	☑	N/A

Legend: ✅ *yes;* ☒ *no;* ☑ *probably, but could not be verified;* ◇ *could not be determined, N/A Not applicable*

2 Overview of key issues addressed

Key Issues Addressed	IPC Federated PIA	PbD PIA F Framework	ICO Handbook V2	ISO	IPC PHIPA	PIA Health and Social Care	BSI RFID PIA
Policy Information (3)	N/A	N/A	☑	N/A	☒	☒	N/A
Methodology	3 phases PIA, guided by the Global Privacy Standard (5)	Guided by the PbD Principles (6)	5 phases PIA (7)	4 steps PIA (8)	Answering the questionnaire as a self-assessment tool	4 stages PIA (9)	6 steps PIA (10)
Legal Compliance Check (11)	N/A	N/A	☑ (12)	☒	N/A	☒	☒
Data Protection Targets	☒	☒	☒	☒	☒	☒	☑ (13)
PIA Report available for the DPA	N/A	N/A	☑	N/A	N/A	☑	☑ (14)
PIA Report Public	N/A	N/A	N/A	N/A	N/A	Recommended, but not mandatory	☒
Stakeholders involvement	N/A	N/A	☑	N/A	N/A	☒	☑
Privacy risk scale	☒	☒	☒	☑ (15)	☒	☒	☑ (16)
Privacy risk treatment	N/A(17)	N/A(17)	☒	☑	☒	☒	☑

Key Issues Addressed	IPC Federated PIA	PbD PIA F Framework	ICO Handbook V2	ISO	IPC PHIPA	PIA Health and Social Care	BSI RFID PIA
Mandatory PIA	N/A	N/A	☒	N/A	N/A	☒	☑ (18)
Possible attackers	☒	☒	☒	☒	☒	☒	☒

Legend: ☑ yes; ☒ no; ✓ probably, but could not be verified; ◇ could not be determined, N/A Not applicable

1. PHIPA defines a “health information custodian” as a person or organization who has custody or control of personal health information.

2. This questions are divided in three sections: 1) PIA screening questions, 2) Data protection Act compliance checklist and 3) Privacy and Electronic Communications Regulations checklist (this third section may include another privacy laws).

3. This 11 questions constitute an initial threshold assessment, to determine whether its potential privacy impact necessitates a PIA. In the other PIA stages there a proposed questions for different items.

4. Following Martin Rost’s classification: Policy A: almost only marketing, Policy B: seeking highest data protection (legal and technical) compliance, and Policy C: for research purposes.

5. The three phases are:

- Information Lifecycle
- Operational Principles
- Implementation

The Global Privacy Standards are available at http://www.ipc.on.ca/images/Resources/gps.pdf.

6. The seven PbD principles are:

1. Proactive not Reactive – Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive Sum, not Zero-Sum
5. End to End Security – Full Cycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it Individual and User-Centric

The Framework discusses the application of the seven PbD Principles in three areas:

1. Information technology;
2. Accountable business processes,
3. Physical design and networked infrastructure

7. Conducting the PIA Process

1. Preliminary phase, to ensure the PIA to be conducted effectively and efficiently.
2. Preparation phase, suggested deliverables are a stakeholder analysis, a consultation strategy and plan, and establishment of a PIA Consulting Group (PCG).
3. Consultation and analysis phase(s) with the framework in place this phase focuses on consultations with stake holders, risk analysis, the recognition of problems, and the search of solutions.
4. Documentation phase. The suggested deliverable is a PIA Report.
5. Review and audit phase, the purpose of this phase is to ensure that the design features arising from the PIA are implemented and are effective.

8. The four steps are:

1. System description

2. Privacy risk identification
3. Privacy impact analysis
4. Privacy impact evaluation

9. The four stages are:

1. PIA threshold management
2. Identification of risks
3. Addressing the risks
4. The PIA Report

10. The six steps are:

1. Characterization of the Application
2. Definition of Privacy Targets
3. Evaluation of Degree of Protection Demand for each Privacy Target
4. Identification of Threats for each Privacy Target
5. Identification and Recommendation of Controls Suited to Protect against threats
6. Assessment and Documentation of Residual Risks

11. For our purposes, this issue means not only asking if the organization is legal compliant, but truly checking its legal compliance with a specific check.

12. Surprisingly, the legal compliance check should be done after the full or small scale PIA, we think the right way would be to check this point in the preparation phase.

13. Privacy targets as defined in the PIA Framework:

1. Safeguard of quality of personal data

2. Legitimacy of processing personal data
3. Legitimacy of processing sensitive personal data
4. Compliance with the data subject’s right to be informed
5. Compliance with the data subject’s right to access, correct and erase data
6. Compliance with the data subject’s right to object
7. Safeguard of confidentiality and security of processing
8. Compliance with notification requirements
9. Compliance with data retention requirements

14. The signed PIA Report that contains an approved resolution, excluding proprietary information not pertinent to the PIA, should be made available to the competent authority at least 6 weeks before deployment.

15.

- Impact of a privacy breach, using 1 for “low impact”, 2 for “medium impact”, 3 for “high impact” and 4 for “very high impact”.
- Likelihood for the privacy risk to happen, using 1 for “very unlikely”, 2 for “unlikely”, 3 for “likely” and 4 for “very likely”.

16. Following BSI baseline criteria:

- Low: the impact of any loss or damage is limited and calculable
- Medium: the impact of any loss or damage is considerable
- High: the impact of any loss or damage is devastating

17. Both documents mention Risk Assessment, but do not explain which kind of risk treatment they recommend.

18. The European Commission’s recommendation indicates that all RFID operators should assess the impact of their operations on privacy and data protection.

Chapter 4

Our Proposed Methodology

In this document we propose a methodology based on the work of Bock/Rost[20].

4.1 Systematic Basis

Our proposed methodology delivers a framework that enables assessing the severity of risks and the adequacy of the countermeasures to mitigate these risks. Therefore, we chose a risk-based approach, taking into account that a DPIA should derive from the impact a data loss or compromise could have at the concerned data subject.

A comprehensive assessment methodology should be as universal as possible to be applied to any kind of process involving personal data. Hence, the success criteria for any kind of Privacy or Data Protection Impact Assessment are verifiability, comparability and transferability.

- Verifiability:
  The results of the assessment have to be verifiable and reproducible to allow for third party auditing or the control of the competent Data Protection Authority (DPA).
- Comparability:
  Results should be comparable to allow customers and public authorities to evaluate the adequacy of different solutions.
- Transferability:
  To minimize the organizational overhead of such an assessment the results should not be a one-time solution but be comparable and applicable to future similar processes and risks.

4.2 Outcome

Our approach fits within PIA Policy B (see above: Section 3.9): The purpose is to conduct intensive assessment of the project in question, taking into account the risks for the affected data subjects.

The outcome will be oriented on the degree of compliance with data protection regulations, although the proposed DPIA is not a purely legal assessment of compliance. The adequacy of legally required technical, organizational and contractual security measures is seldom a yes or no-question. The law being technology-neutral gives sufficient flexibility to data controllers and data processors to install a variety of security measures. Therefore, a Data

[20] Martin Rost, Kirsten Bock: *Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen* (translated: *“Privacy by Design and the New Protection Goals – Principles, Goals, and Requirements“*), in: Datenschutz und Datensicherheit (DuD), 35(1):30-35, 2011.

Protection Impact Assessment does not stop at the written law but needs to establish universal criteria to evaluate whether data protection risks are sufficiently mitigated.

The outcome of such an assessment is a written report on the results stating the risks and if and how they are addressed and if this is sufficient with regard to data protection requirements. This report is neither a full legal risk assessment, because other legal questions like liability or compliance are being left out, nor a business risk assessment, because it does not address cost/benefit-balancing. But it is the basis upon which further assessments of legal compliance or business risks may be conducted.

4.3 Concept

4.3.1 Subject: Personal Data, Systems, and Processes

The subject of a DPIA is not limited to personal data. In fact security measures only directly applied to the data would fall short. To adequately address the data protection impact of a project or application one needs to evaluate the full picture and take into account not only technical but also organizational and contractual safeguards. Technical measures respectively may be applied on the layer of "**data**" (software) or on the layer of **IT systems** (platform and infrastructure). Additionally, the more abstract concept of **processes** (this includes technical as well as organizational processes) allows assessing the risks of the complete project. Therefore, a comprehensive methodology has to address at least three different subjects: data, systems and processes.

4.3.2 Gradation: Level of Required Protection

Not every set of data or every process has the same sensitivity. The processing of names and email addresses of professional contacts within a Customer Relationship Management application poses significantly less risk to the data subjects than a database of patients undergoing a cancer treatment. Hence, the more sensitive data or processes are, the more safeguards they need.

Therefore, it makes sense to classify data and processes into categories regarding their required level of protection. For this classification we need to take into account not only the sensitivity of the data itself (Art. 8 of the Data Protection Directive 95/46/EC mentions categories of sensitive data) but also the impact of possible consequences and damages to an affected data subject in case of loss or corruption.

- **Normal:**
  - The data and/or process are not per se sensitive according to Art. 8 95/46/EC
  - Possible consequences for the data subject would be manageable or limited
  - Possible damages could be compensated or are reversible
- **High:**
  - Possible consequences could have substantial impact on the data subject (e.g. influence on behaviour, social life or participating in society
  - Possible damages could be compensated with increased use of resources and effort
- **Very high:**
  - Possible consequences are severe to existential for the data subject
  - Possible damages are irreversible and cannot be fully compensated

This coarse classification allows evaluating the adequacy of safeguards, as not all projects and processes need to address the highest risk category. In many cases fewer or other data protection measures may be sufficient.

4.3.3 Criteria: Protection Goals

Key element for our methodology is the establishment of six principles, so called “Protection Goals”. These Protection Goals serve as benchmarks to suggest appropriate countermeasures or to measure the adequacy of existing countermeasures and data protection safeguards.

4.3.3.1 IT Security Goals

To determine which measures are adequate, system designers commonly rely on conventional methods of IT security risk assessments. In this context, three classical IT security goals are commonly used to ascertain which risks are inherent in designing, deploying, maintaining and providing specific services. In doing so, it can be assessed which countermeasures are fit to eliminate or at least diminish these risks. These three classical IT security goals are:

- Confidentiality
- Integrity
- Availability

In relation to digital services of all kinds, these three different goals (also called “Classic CIA Triad”) help to structure risks and determine appropriate countermeasures. Moreover, they are a useful tool to set up an effective Information Security Management System (ISMS). Elements of such a system may for instance be the standards ISO/IEC 27001, ISO/IEC 27002, COBIT (Control Objectives for Information and related Technology) and ITIL (Information Technology Infrastructure Library). However, these three classical IT security protection goals are not always in complete balance while following their core principles. Indeed, it is fact that there is no "one size fits all solution". Instead, an analysis of the individual use case itself is required. Thereby, it must be determined to which extent which goal can be pursued and which balance can be found once some single goals conflict with each other.[21]

4.3.3.2 Data Protection Goals

Beyond the scope of these classical IT security protection goals, the protection of individuals’ personal data demands another perspective from the viewpoint of the concerned persons, i.e. citizens, customers, employees, users, and patients. This viewpoint complements the aspects of classical IT security with additional demands shaped through the legal requirements of personal data protection. These demands can be expressed into new specific protection goals (“Data Protection Goals” or “Privacy Protection Goals”) also fit for the detection of protection loopholes, mismatches, and appropriate methods of resolution. These new data protection-specific goals are:

- Unlinkability
- Transparency
- Intervenability[22]

[21] Martin Rost, Andreas Pfitzmann: *Datenschutz-Schutzziele – revisited*, in: Datenschutz und Datensicherheit (DuD), 33(6):353-358, 2009.

[22] Martin Rost, Kirsten Bock: *Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen* (translated: *“Privacy by Design and the New Protection Goals – Principles, Goals, and Requirements“*), in: Datenschutz und Datensicherheit (DuD), 35(1):30-35, 2011.

4.3.3.2.1 Unlinkability

Each processing of personal data is only lawful on the basis of a certain purpose determined in advance. This can be derived from Art. 6 para. 1 (b) of Directive 95/46/EC stating that personal data must be *“collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”*. Consequently, this means that personal data which is being processed for one purpose should not be linked to other personal data being processed for another purpose and thus outside the scope. At least, the implementation of such linkage of differently purpose-bound data sets should not be possible without disproportionate effort. The objective is to prevent misuse and profiling spanning across contexts. Thus, Unlinkability is a protection goal that aims at the enforcement of strict purpose-binding regarding the processing of personal data as well as at data minimization. In doing so, it prevents the misuse of personal data for originally unintended purposes. This preconditions the knowledge of thematically related processes and contradicting purposes. Potential measures to realise Unlinkability can be the separation of data parts and a clear conception of technical work processes. Moreover, a distinction between different roles of involved parties and unequivocal responsibility allocation prior to the initiation of data collection and processing can be useful in enabling Unlinkability.

4.3.3.2.2 Transparency

Transparency means that all involved parties should be able to fully understand the legal, technical, and organizational conditions related to the processing of the personal data in question. This foremostly concerns the data subject, but is also relevant for operators, supervisory authorities and other concerned entities involved. The necessary information may be conveyed in law directly or in the contracts between parties. Either way, the aim should be to achieve clarity regarding the scope and conditions of the personal data usage so it can be comprehended and verified with reasonable effort. In this context, easy to understand Privacy Policies are also a key factor as well as an effortlessly understandable communication which technologies are used and which organizational processes and responsibilities are put in place. Regarding the processing of the personal data itself, the specifics of the processing operation, such as normal flow, location, transmission details, recipients and potential data protection risks should be included. Supplementary aspects to enhance knowledge would be the implementation of appropriate logging, documentation, and effective data protection management systems like access authorisation and corresponding access control. Changes in the data stock (e. g. additions, modifications, deletions) must be documented and made visible in some way. Thus transparency must be realised not only at the stages of the data processing, but throughout the whole lifecycle of the data (collection, storage, processing, and deletion).

Transparency is a foundation protection goal to the two other goals Unlinkability and Intervenability. Unlinkability as a goal comprising the data minimization and need-to-know principle is reliant on transparency to allow an appropriate assessment of the necessity of the processing operation in question. To serve Unlinkability, transparency should be achieved by categorising types of personal data processed, naming the purposes making the processing necessary, and documenting processing duration, data retention, and deletion periods. Intervenability is another protection goal reliant on transparency owing to the fact that the control over a processing operation is dependent on knowledge and overview over said operation. This is especially important with regard to the data subject’s viewpoint, enabling her to exercise her lawful rights, as elaborated in the section about Intervenability.

4.3.3.2.3 Intervenability

Intervenability means the effective provision of ways to intervene in personal data processing within the boundaries of the rights and obligations as codified in the EU Data Protection Directive 95/46/EC. This includes not only the possibility for the data subject to exercise her rights, but also the operational access to or influence on processes for data subjects, data controllers, or supervisory authorities to ensure the enforcement of lawful data processing. Regarding the data subject's rights, this concerns an easy insight into which personal data is processed about her. Moreover, she must be able to exercise her rights corresponding to the requirements of the European Data Protection Directive. These rights are:

- Notification of processing, or changes thereof
- Access to the own personal data
- Modification modalities with regard to this data
- Erasure/rectification modalities with regard to this data
- Modalities to express, withhold, or withdraw informed consent to the processing

Measures to realise Intervenability for data subjects can be functional features of the system to upload, modify (rectify), blank, or delete own personal data. Moreover functions, to express and document the grant, withhold, or withdrawal of consent, as well as objections to unauthorised processing. For other entities, such as the service providers, or supervisory authorities, own control features can be implemented. Such can be the possibility to terminate a process, or to trigger a revocation of a process which has been erroneously initiated.

4.3.3.3 Interplay

The Protection Goals are in a bilateral field of tension. Two Protection Goals at a time can be seen as opposite poles on a graph. The field of tension results from the fact that respectively only one Protection Goal can be 100% fulfilled while the other is necessarily partly neglected. In this field of tension it is impossible to fulfil two opposing Protection Goals 100%.

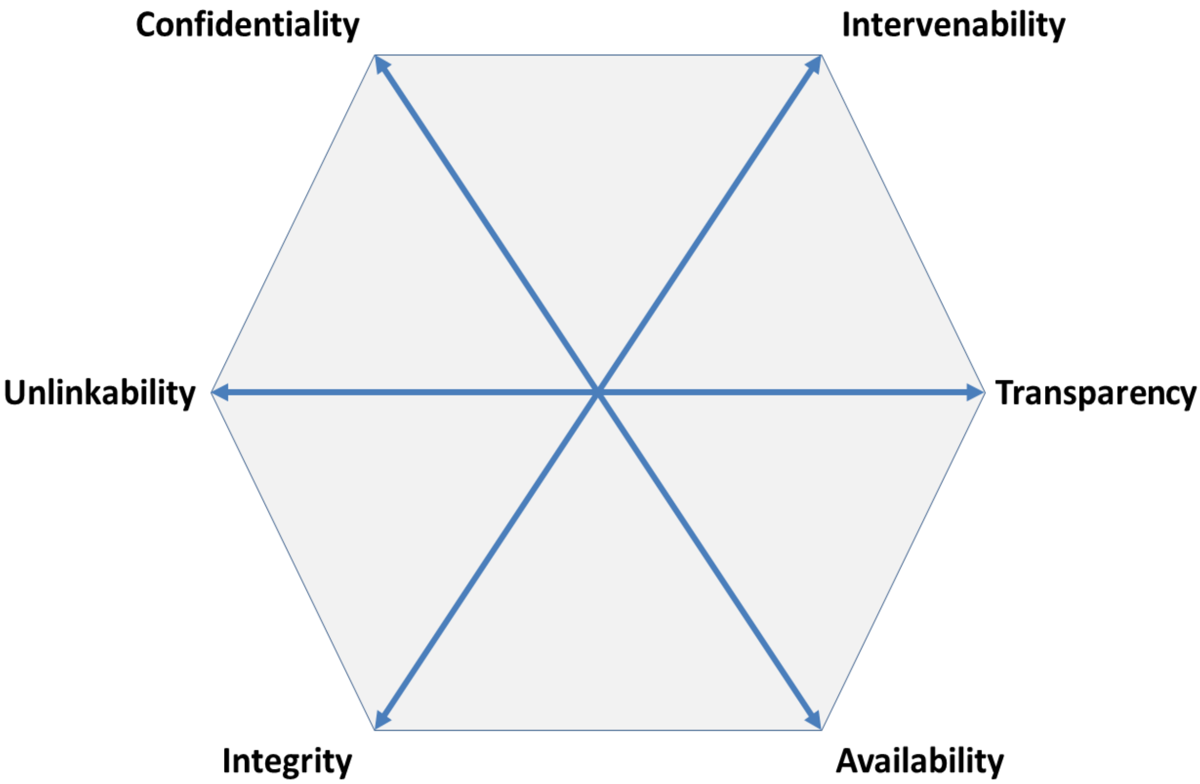

Figure 2: Interplay of Protection Goals

The six Protection Goals form three of these opposing graphs.

- Confidentiality and Availability
- Integrity and Intervenability
- Transparency and Unlinkability

To give a plain example: On the one hand, full availability would mean that everyone from everywhere with every device would have access to a specific document, ergo no confidentiality. On the other hand complete confidentiality would mean that no one has access to the document, ergo no availability. In a real world example neither of these two extremes would be desirable. In most cases it is necessary to carefully balance these two Protection Goals to achieve the optimal design. The more sensitive the document is, the more the scale is in favour of confidentiality. Hence appropriate measures need to be installed to safeguard the confidentiality, while also allowing the competent persons to access the document.

Consequently, the use of Protection Goals depends on the subject of the assessment and its sensitivity with regard to personal data.

4.3.4 Assessment: Analysis, Balancing, and Evaluation

The actual assessment can be described in four steps:

1. **Analysis of the actual status**
   The actual assessment starts with analyzing the project or process in question in detail and identifying data, IT systems and (sub-)processes.

2. **Determination of required level of protection (data subject's point of view)**
   Depending on several different attacker models (data subject, user, administrator, government, third party) potential risks for the data subjects need to be identified and evaluated according to our classification of required protection levels, normal, high and very high.

3. **Balancing of Protection Goals**
   Next step is to evaluate which Protection Goals need to be addressed to which degree to mitigate the identified risks. Therefore the Protection Goals need to be weighed and balanced for each subject (data, IT systems and processes).

4. **Assessment of data protection measures and security safeguards**
   In this last step the existing technical, organizational and contractual measures need to be analyzed and measured against the Protection Goals and identified risks. The outcome can either be that a risk regarding a Protection Goal is sufficiently addressed or that there is a remaining gap regarding the safeguards. In this case, based on the Protection Goals adequate measures can be proposed.

4.3.5 Excursus: Catalogue of Safeguards

The proposed methodology allows creating a reference catalogue of generic security measures. This catalogue can be used to compare and evaluate the outcome of a case-by-case DPIA. Or it may serve as a first overview in case a data controller wants to orientate himself and plan a future project.

This reference catalogue leads to security measures in 54 fields.

	3 subjects (data, IT systems, processes)
x	3 protection levels (normal, high, very high)
x	6 protection goals
=	54 fields of data protection measures

To enhance its comprehensibility we limit our example table to two factors: subjects and protection goals.

Table 1: Catalogue of Safeguards

Catalogue of Safeguards[23]	Data	Systems	Processes
Availability	Limitation of rights to change/delete Protection against malware Back up of data	Protection against malware Back up of configuration and software Hardware redundancy Back up network	Stand-in personnel Available documentation Planning for emergency cases
Confidentiality	Limitation of access/reading rights	Limitation of reading access to IT systems (e.g. network	Confidentiality duties by contract (personnel, sub-

[23] Based on Thomas Probst: *Generische Schutzmaßnahmen für Datenschutz-Schutzziele* (translated: *"Generic Data Protection Measures for Data Protection Goals"*), in: Datenschutz und Datensicherheit (DuD), 36(6), 2012, p. 443.

Catalogue of Safeguards[23]	Data	Systems	Processes
	Logging of access Encryption (including secure key management) End-to-end encryption	separation by security gateway) Encryption on infrastructure layer Multi-tenancy	contractors) Concept of roles (who needs to have access?)
Integrity	Limitation of writing rights Logging of writing access/changes Notification of changes Technical controls of integrity (e.g. signatures, hashes)	Limitation of configuration rights Protection against malware Byzantine fault tolerance/ comparison of back ups Periodic control/audits	Detailed Planning of processes Systematic distribution of rights Change management procedures Regular quality audits
Unlinkability	Deletion, when no longer necessary Limitation of usage Data segregation Anonymization Pseudonymization Sticky Policies	Segregation of data bases Limitation of use/transfer functionalities on system layer Separation on system layer Multi-tenancy Physical separation of infrastructure	Separation of processes Division of powers/ rights Separation of processes into steps (different responsible entities for these steps)
Transparency	Documentation Documentation of necessity for processing Auditable logging (insuring integrity)	Documentation of systems Logging of changes to configuration Monitoring	Privacy Policy (comprehensive and in clear language) Clear documentation Role concept
Intervenability	Enabling of necessary data fields (e.g. right to reply, demand to correct)	System functionalities for blanking, deletion, correction, replies Functionalities for notice, choice and consent Possibility to shut down subsystems Possibility to override automated decisions	Management of addressing data subject's rights Single point of contact for data protection questions Self-management options for the data subject Change management

4.4 Necessary Adaption for the TClouds Scenarios

The challenge we face when applying this universal DPIA methodology to the TClouds use case scenarios is that we do not have complete and running products. The TClouds benchmark applications are test beds for the TClouds infrastructure but do not include written organizational policy responsibilities or contracts between different actors yet. Even the technical implementation may be incomplete compared to an actual future product.

Therefore, we are not able to assess the complete picture based on technical, organizational and contractual measures. Our DPIA has to address an earlier stage of product development, where we need to identify the risks, assess the adequacy of technical countermeasures in place, and suggest organizational and contractual countermeasures and additional technical means to fill in the remaining gaps.

Wherever the TClouds components or architecture offer a significant or measurable privacy or security benefit, we will visualize it by including a Kiviat diagram.

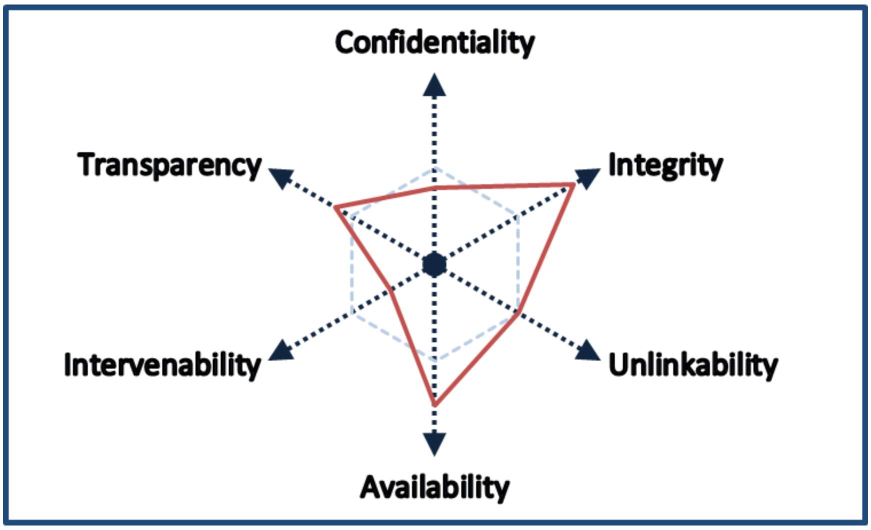

Figure 3: Example Data Protection Goals Kiviat Diagram

This diagram will compare a normal implementation on a basic commodity cloud (grey line) with the integration of TClouds solutions (red line). The growing or shrinking of the figure's face makes benefits and drawbacks regarding the data protection goals easily visible.

Disclaimer: The next chapters of this deliverable have been marked as "confidential" since they directly deal with internal TClouds results. Therefore, this public version of the deliverable jumps directly to the last chapter "Outlook" without going into detail of applying the developed Data Protection Impact Assessment methodology to TClouds components and discussing different levels of protection goals by means of Kiviat Diagrams.

Chapter 5

Outlook

The DPIA methodology elaborated in this deliverable has been successfully applied to the TClouds use cases and the infrastructure components involved. The part of the actual assessment has been attributed as “confidential” in TClouds’ Document of Work. Therefore it does not belong to the public part of this deliverable.

Still, it is noteworthy to mention a few lessons learned: Firstly, the available schemes for Privacy Impact Assessment or Data Protection Impact Assessment differ significantly, and even in a to-be-further-harmonized regime of the European Data Protection Framework effort is needed to standardize the DPIA methodology or find other ways to compare the results stemming from the application of various approaches. As one overarching scheme, working with six protection goals (confidentiality, integrity, availability, unlinkability, transparency, intervenability) has turned out as a reasonable solution for DPIA.

In TClouds, the potential privacy impact of the home healthcare scenario due to the sensitiveness of medical data is much greater than of the smart lighting scenario. This is reflected by the degree of how far the individual protection goals have to be fulfilled. In the full version of this deliverable, various Kiviat diagrams have been provided that visualize to which extent the protection goals can be achieved by using certain TClouds components. Although a full DPIA is only possible for mature products, several assessments were feasible with respect to the available versions. This shows the potential use of both the developed DPIA methodology and the elaborated TClouds components. For example, fragmentation, pseudonymization, and encryption support the objective of the unlinkability protection goal; transparency is fostered by logging functionality as well as user information and contracts, and intervenability is provided by a user-centric approach.

Finally, the cloud-of-clouds deployment supports availability and integrity, but – as it had been pointed out in previous deliverables – also may enhance the level of privacy and data protection, thereby promoting the other protection goals as well. Further research in this field would be of great help in designing cloud systems compliant with data protection law and privacy principles.

Chapter 6

Bibliography

6.1 EU and Article 29 Working Party

- Article 29 Working Party: Working Document on the processing of personal data relating to health in electronic health records (HER), WP131, adopted on 15 February 2007.
- Article 29 Working Party: Opinion 4/2007 on the concept of personal data, WP136, adopted on 20 June 2007.
- Article 29 Working Party: Opinion 1/2010 on the concepts of data controllers and data processors, WP169, adopted on 16 February 2010.
- Article 29 Working Party: Opinion 12/2011 on smart metering, WP183, adopted on 4 April 2011.
- Article 29 Working Party: Opinion 15/2011 on the definition of consent, WP187, adopted on 13 July 2011.
- European Commission: Recommendation on preparations for the roll out of smart metering, Brussels, 9 March 2012, COM (2012) 1342 Final.
- Phil Walker, Department of Health (England), Comments on the draft of WP131 of the Article 29 Working Party, http://ec.europa.eu/justice/policies/privacy/docs/health_records/member_states/dept_health_uk_en.pdf.

6.2 Research Papers

- Kirsten Bock, Martin Rost: *Impact Assessment im Lichte des Standard-Datenschutzmodells*, in: Datenschutz und Datensicherheit (DuD), 36(10):472-477, 2012.
- Luigi Catuogno, Alexandra Dmitrienko, Konrad Eriksson, Dirk Kuhlmann, Gianluca Ramunno, Ahmad-Reza Sadeghi, Steffen Schulz, Matthias Schunter, Marcel Winandy Jing Zhan: *Trusted virtual domains – design, implementation and lessons learned*, in: Proceedings of the First international conference on Trusted Systems, pp. 156-179, Egham, UK, 2009.
- Roger Clarke: *Privacy impact assessments*. Xamax Consultancy Pty Ltd., Version of 19 April 1999, with small revisions subsequently, and progressive enhancements to the Bibliography, most recently 26 May 2003, http://www.rogerclarke.com/DV/PIA.html.
- Ludwig Edelstein: *The Hippocratic Oath*, Supplement to the Bulletin of the History of Medicine, No. 1, Baltimore: Johns Hopkins University Press, 1943.
- Pascal Hahulla: *Datenschutzfreundliche Konzeptionierung von Smart Grid und Smart Metering* (translated: *"Data protection friendly conceptioning of Smart Grid and Smart Metering"*), published 9th August 2010, http://pascal.hahulla.de/studium/Konzeptionierung-SG-SM.pdf

- Rainer Knyrim, Gerald Trieb: *Smart metering under EU Data Protection Law*, in: International Data Privacy Law, Vol. 1, No. 2, 121, 2011.
- Leslie Lamport, Robert Shostak, Marshall Pease: *The Byzantine Generals Problem*, in: ACM Transactions on Programming Languages and Systems, Volume 4 Issue 3, July 1982, pp. 382-401, ACM New York, NY, USA.
- Klaus J. Müller: *Gewinnung von Verhaltensprofilen am intelligenten Stromzähler* (translated: *"Extraction of behavior profiles by the intelligent smart meter"*), in: Datenschutz und Datensicherheit (DuD), 34(6):359-364, 2010.
- Thomas Probst: *Generische Schutzmaßnahmen für Datenschutz-Schutzziele* (translated: *"Generic Data Protection Measures for Data Protection Goals"*), in: Datenschutz und Datensicherheit (DuD), 36(6): 439-444, 2012.
- Martin Rost, Andreas Pfitzmann: *Datenschutz-Schutzziele – revisited*, in: Datenschutz und Datensicherheit (DuD), 33(6):353-358, 2009.
- Martin Rost, Kirsten Bock: *Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen* (translated: *"Privacy by Design and the New Protection Goals – Principles, Goals, and Requirements"*), in: Datenschutz und Datensicherheit (DuD), 35(1):30-35, 2011.
- Bruce Schneier, John Kelsey: *Secure audit logs to support computer forensics*, in: ACM Transactions on Information and System Security (TISSEC), Volume 2 Issue 2, May 1999, pp. 159-176, ACM New York, NY, USA.
- Adi Shamir: *How to share a secret*, in: Communications of the ACM, Volume 22, 1979, pp. 612-613, ACM New York, NY, USA.
- David Wright, Paul de Hert: *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

6.3 URL Index

- PIAF EU Project, Final Deliverable http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- Intel Corp.: OpenAttestation SDK (OAT), an SDK for Remote Attestation. https://github.com/OpenAttestation/OpenAttestation
- http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf
- http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf
- http://www.aerzteblatt.de/archiv/31932
- http://www.aerzteblatt.de/archiv/31932
- http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm369431.htm
- http://www.hiqa.ie/publications/guidance-privacy-impact-assessment-health-and-social-care
- http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx
- http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
- http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

- http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf
- http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf
- https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.pdf?__blob=publicationFile
- https://www.datenschutzzentrum.de/guetesiegel/Privacy_Protection_Goals_in_privacy_and_data_protection_evaluations_V05_20120713.pdf
- https://www.datenschutzzentrum.de/material/themen/gesund/patdvia.htm
- https://www.european-privacy-seal.eu/results/articles/BockRost-PbD-DPG-en.pdf