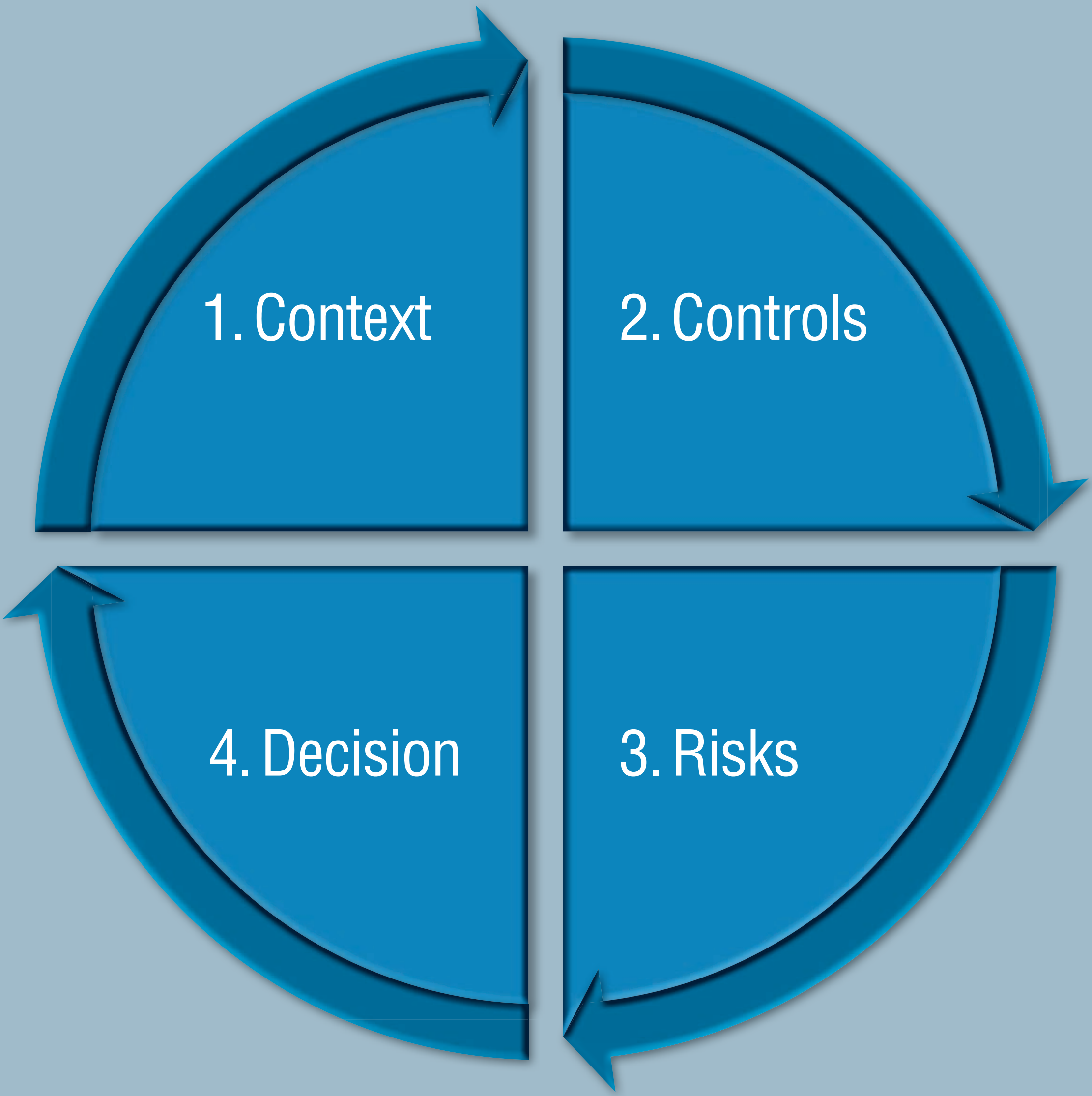
PRIVACY IMPACT ASSESSMENT (PIA)

Methodology (how to carry out a PIA)



CNIL
Commission Nationale de l'Informatique et des Libertés

June 2015 Edition

Contents

Foreword

This document must be used in conjunction with the following guides:

- [PIA-2-Tools], which includes models and knowledge bases for the practical application of this methodology;
- [PIA-3-GoodPractices], which is a catalog of controls designed to comply with legal requirements and treat the risks assessed using this methodology.

Writing conventions for all of these documents:

- the term “privacy” is used as shorthand to refer to all fundamental rights and freedoms (including those mentioned in Articles 7 and 8 of the [EUCharter], Article 1 of the [Directive-95-46] and the Article 1 of the [DP-Act]: “human identity, human rights, privacy, or individual or public liberties”);
- the acronym “PIA” is used interchangeably to refer to *Privacy Impact Assessment* (PIA) and *Data Protection Impact Assessment* (DPIA);
- wordings in brackets ([text]) correspond to references.

Introduction

A PIA rests on two pillars:
1. fundamental principles and rights, which are "non-negotiable", established by law and which must be respected and cannot be subject to any variation, regardless of the nature, severity and likelihood of risks;
2. management of data subjects' privacy risks, which determines the appropriate technical and organizational controls to protect personal data.

Scope

This document explains how to carry out PIAs. It describes how to use the [EBIOS][1] method in the specific context of "Personal Data protection".

It is intended for data controllers who wish to demonstrate their compliance approach and the controls they have selected (concept of *Accountability*), as well as for product providers wishing to show that their solutions do not breach privacy thanks to a design that respects privacy (concept of *Privacy by Design*)[2]. It is useful to all stakeholders involved in creating or improving processing of personal data or products:

- ❑ decision-making authorities who commission and validate the creation of new processings of personal data or products;
- ❑ project owners, who must conduct an assessment of risks to their system and define the security objectives;
- ❑ prime contractors, who must propose solutions to treat risks pursuant to the objectives identified by project owners;
- ❑ data protection officers (DPO), who must support project owners in the area of personal data protection and decision-making authorities;
- ❑ chief information security officers (CISO), who must support project owners in the area of information security (IS).

[1] EBIOS – *Expression des Besoins et Identification des Objectifs de Sécurité* (Expression of Needs and Identification of Security Objectives) – is the name of the risk management method published by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI, the French National Cybersecurity Agency).

[2] In the rest of the document, the term "processing of personal data" is interchangeable with the term "product".

Why conducting a PIA?

A PIA can be carried out on any complex or innovative processing of personal data or product whose stakes are high. There may also be a legal obligation to carry out a PIA.

Personal data can be valuable for the organization that processes them. But their processing *de facto* creates a significant liability due to the risks brought upon the privacy of data subjects.
Personal data have value for data subjects as well. They can be useful for administrative or commercial purpose, or may even contribute to their image. But security breaches in data protection can also cause physical injury, material and moral damage.
Finally, personal data have a value for others. This includes a market value if they are exploited for commercial purposes (spam, targeted advertising, etc.), or a nuisance value in the case of unfair actions (discrimination, denial of access to benefits, etc.) or malicious actions (fraudulent bank transaction, identity theft, blackmail threatening to destroy data, burglary, defamation, threats, assault, etc.).

Moreover, we can see phenomena that tend to change our view of threats: a culture of exposing our private life without worrying about the impacts this could have on our professional and social future, as well as increased capabilities of risk sources (generation Y, structured criminal organizations and powerful tools easily found on the Internet, espionage between states, etc.). Personal data are therefore all the more vulnerable.

Given the stakes that are often high, and the evolution of systems[3] and threats, risk management enables to determine the necessary and sufficient controls. It makes it possible to methodically study the processings of personal data or products, prioritize risks and treat them in a proportionate manner in order to optimize costs and make decisions on the basis of information made as objective as possible.

Finally, a PIA helps demonstrating the implementation of privacy principles so that data subjects retain control of their personal data.

[3] Information systems, telephone, paper channels, organizational or interpersonal.

What is a privacy risk?

A risk is a hypothetical scenario that describes:

- how risk sources (e.g. an employee bribed by a competitor)
- could exploit the vulnerabilities in personal data supporting assets (e.g. the file management system that allows the manipulation of data)
- in a context of threats (e.g. misuse by sending emails)
- and allow feared events to occur (e.g. illegitimate access to personal data)
- on personal data (e.g. customer file)
- thus generating impacts on the privacy of data subjects (e.g. unwanted solicitations, feelings of invasion of privacy, etc.).

The following diagram summarizes all the concepts above:

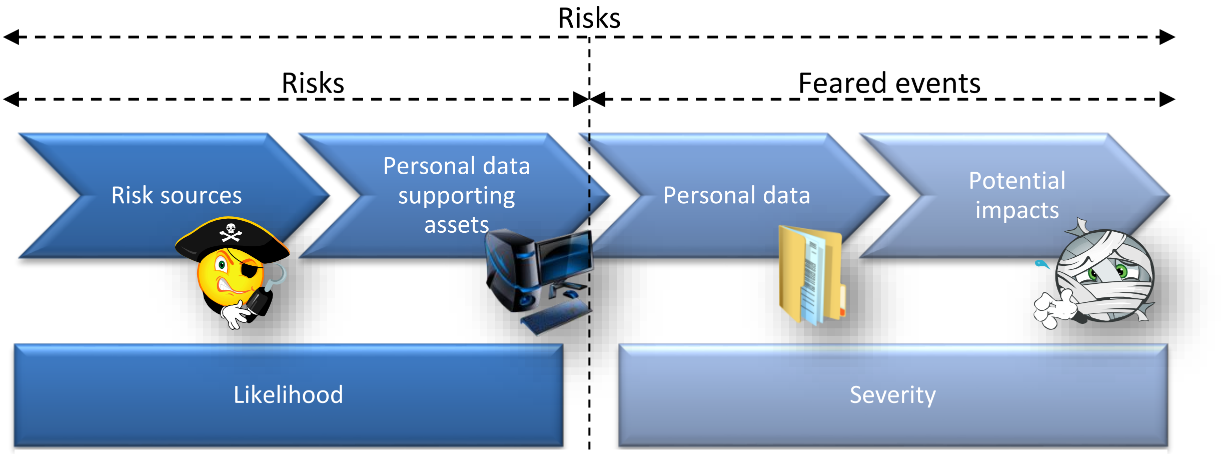


Figure 1 – Risk components

The risk level is estimated in terms of severity and likelihood:

- **severity** represents the magnitude of a risk. It essentially depends on the prejudicial effect of the potential impacts[4];
- **likelihood** represents the possibility for a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing threats and the level of capabilities of the risk sources to exploit them.

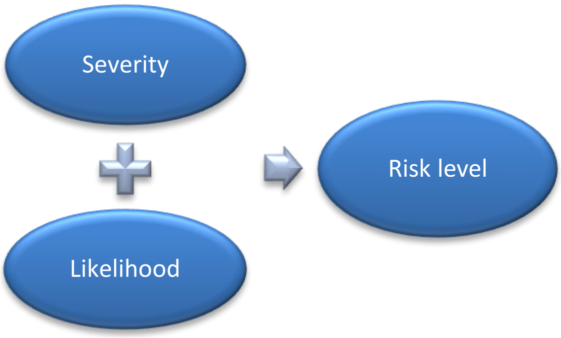


Figure 2 – Factors used to estimate risks

[4] In view of the context of the processing of personal data (nature of data, data subjects, purpose of the processing, etc.).

How is a PIA conducted?

The compliance approach implemented by carrying out a PIA is based on the respect for privacy principles:

- respect for legal principles for privacy protection (specified, explicit and legitimate purpose; adequate, relevant and not excessive data; clear and full information to data subjects; limited retention period; the right of opposition, access, correction and deletion, etc.), to determine and justify the relevance of the controls intended to meet these requirements;
- management of risks related to the security of personal data and having an impact on data subjects' privacy in order to "*take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties*" (Article 34 of [DP-Act][5]).

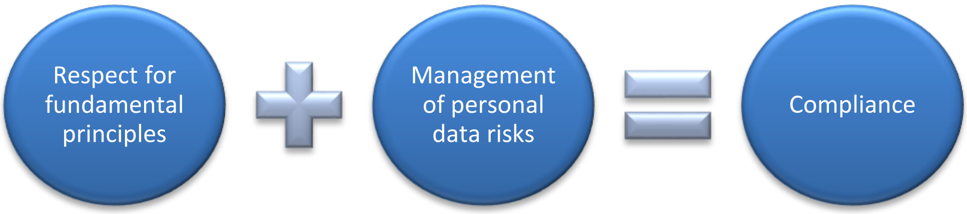

Respect for fundamental principles
Management of personal data risks
Compliance

Figure 3 – Compliance approach using a PIA

In summary, to comply with [DP-Act][6], it is necessary to:

1. define and describe the **context** of the processing of personal data under consideration and its stakes;
2. identify existing or planned **controls** (to comply with legal requirements and to treat privacy risks in a proportionate manner);
3. assess privacy **risks** to ensure they are properly treated;
4. make the **decision** to validate the manner in which it is planned to comply with privacy principles and treat the risks, or review the preceding steps.

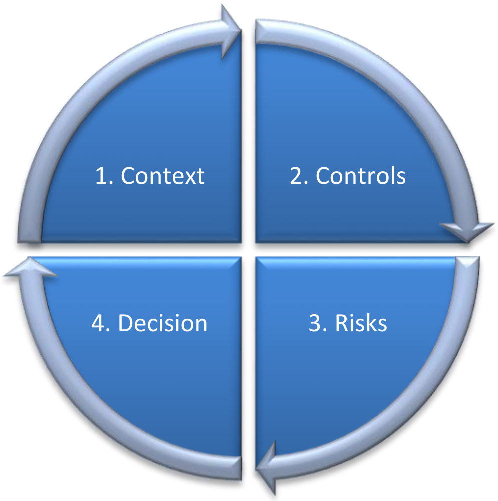


Figure 4 – General approach for carrying out a PIA

This is a continuous improvement process. Therefore, it sometimes requires several iterations to achieve an acceptable privacy protection system. It also requires a monitoring of changes over time (in context, controls, risks, etc.), for example, every year, and updates whenever a significant change occurs.

[5] And Article 17 of the [Directive-95-46].
[6] And with [Directive-95-46].

The following diagram shows the detailed approach:

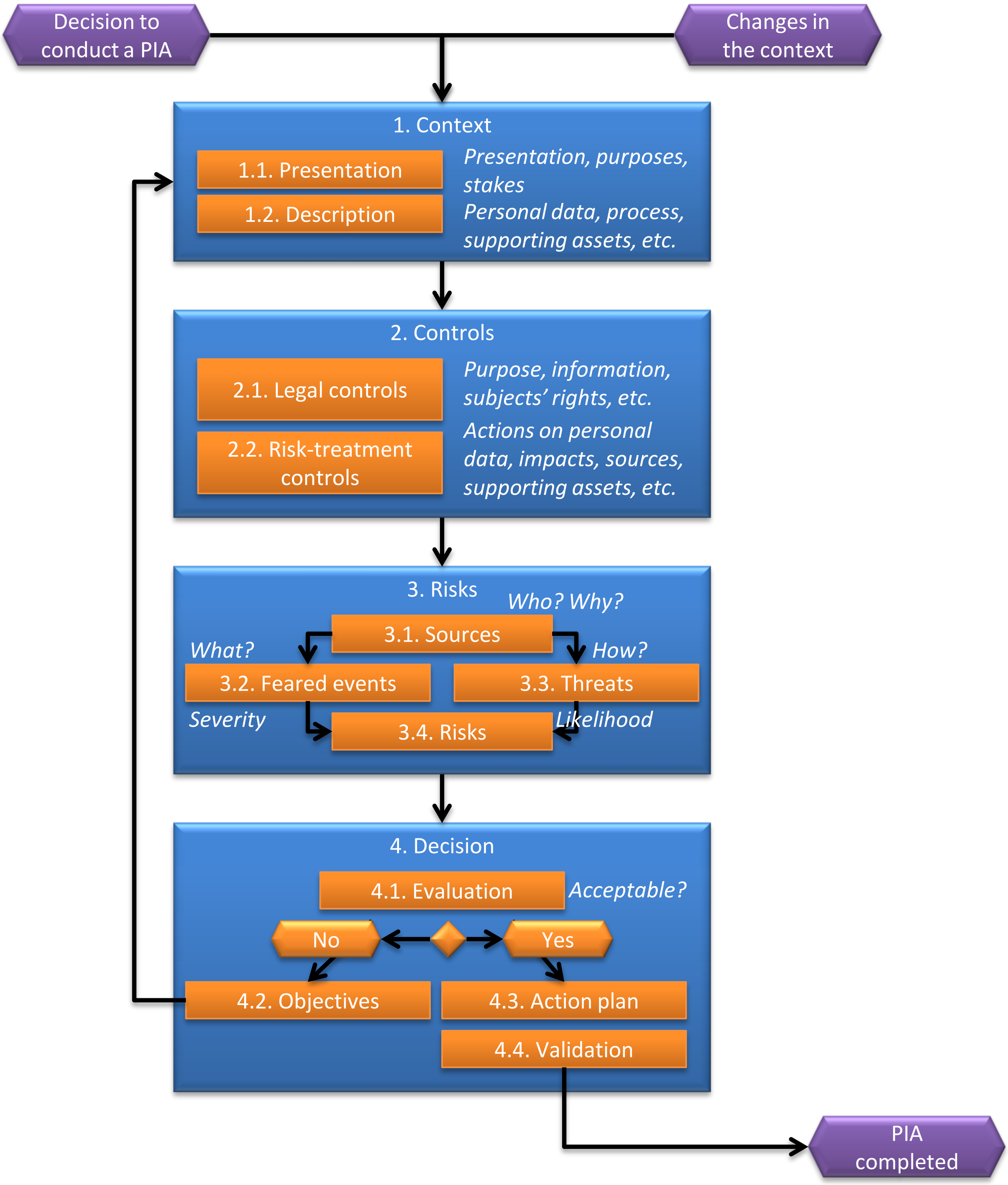


Figure 5 – Detailed approach for carrying out a PIA

<u>The approach should be implemented as soon as a new processing of personal data is designed</u>. Implementing this approach at the outset makes it possible to determine the necessary and sufficient controls and thus to optimize costs. Conversely, implementing it after the creation of the system and the implementation of controls may call into question the choices made.

Who takes part in the PIA?

In general, a PIA is carried out by a data controller or a product provider.

A PIA requires the participation of several stakeholders of the data controller[7], with different roles and responsibilities depending on the steps:

Steps in the methodology	Controller	Project owner[8]	Prime contractor[9]	DPO[10]	CISO[11]
1.1. General description	Accountable[12]	Consulted[13]	Informed[14]	Responsible[15]	Informed
1.2. Detailed description	Accountable	Consulted	Informed	Responsible	Informed
2.1. Legal controls	Accountable	Consulted	Consulted	Responsible	Informed
2.2. Risk-treatment controls	Accountable	Consulted	Consulted	Informed	Responsible
3.1. Risk sources	Accountable	Consulted	Informed	Informed	Responsible
3.2. Feared events	Accountable	Consulted	Informed	Responsible	Consulted
3.3. Threats	Accountable	Informed	Consulted	Informed	Responsible
3.4. Risks	Accountable	Informed	Informed	Responsible	Consulted
4.1. Evaluation	Accountable	Informed	Informed	Responsible	Consulted
4.2. Objectives	Accountable	Consulted	Consulted	Responsible	Informed
4.3. Action plan	Accountable	Responsible	Consulted	Informed	Informed
4.4. Formal validation	Responsible	Informed	Informed	Consulted	Informed

These responsibilities can be adapted to each specific context. They must particularly be adapted to the organization's processes, such as project management. Furthermore, people outside the organization may need to be involved and informed.

[7] The PIA can also be carried out by a processor acting under the responsibility of the data controller.
[8] It refers to business. It may be delegated, represented or subcontracted.
[9] It may also be delegated, represented or subcontracted.
[10] Data Protection Officer, or the person in charge of "Data protection" aspects.
[11] Chief Information Security Officer, or person in charge of "Information Security" aspects.
[12] Person duly authorized to approve the action.
[13] Person(s) consulted to obtain information useful for the action.
[14] Person(s) informed of the results of the action.
[15] Person(s) responsible for carrying out the action.

What is a PIA report?

The PIA report is the document to be produced when a PIA is carried out. It should include at least the following parts:

PIA report

Introduction

- Presentation of the processing of personal data under consideration

Body of the PIA

- Description of the scope
- List of legal controls
- List of risk-treatment controls
- Risk map

Conclusion

- Rationale to validate the PIA

Appendices

- Detailed description of the scope
- Detailed presentation of the controls
- Detailed description of the risks
- Action plan

It must be made available[16] to data protection authorities[17].
It is also sometimes useful to publish and/or distribute all or part of the PIA report[18].

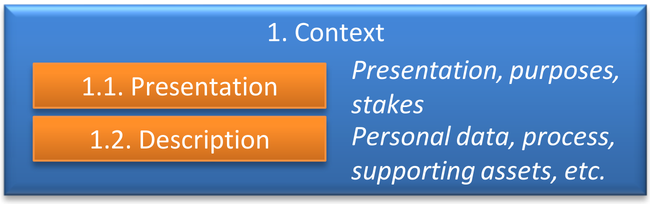
[16] It need not be routinely sent, but must be kept available to authorities which may request it.

[17] In France, the CNIL.

[18] For example, if regulatory obligations so demand, if it is required as element of accountability, or when deemed appropriate for reasons of image.

1. Context: scope of the PIA

Objective: gain a clear view of the processing(s) of personal data under consideration.

Step	Description	Report
	1. Context 1.1. Presentation *Presentation, purposes, stakes* 1.2. Description *Personal data, process, supporting assets, etc.*	❑ Presentation of the processing(s) of personal data under consideration ❑ Description of the scope ❑ Detailed description of the scope

1.1. General description

- ❑ Describe the **processing(s) of personal data** under consideration, its(their) **purposes** and **stakes**[19].
- ❑ Identify the **data controller** and the **processors**.

1.2. Detailed description

- ❑ Define and describe the scope in detail:
  - ○ the **personal data** concerned, their **recipients** and **retention periods**;
  - ○ description of the **processes** and personal data **supporting assets** for the entire personal data life cycle (from collection to erasure).

Tips for carrying out the actions

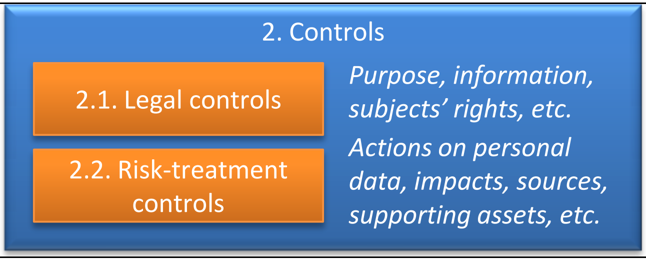
- ❑ Several processings of personal data can be studied in the same study.
- ❑ It is generally useful to consider and distinguish the personal data:
  - ○ those related directly to the processing;
  - ○ those necessary for implementing controls[20].
- ❑ This step should be reviewed every time the context changes.

[19] Answer the question "What are the expected benefits (for the organization, for data subjects, for society in general, etc.)?".

[20] Controls selected to comply with legal requirements (information to subjects, consent, rights of opposition, access, correction and deletion) and to treat the risks (including identity management, access control and logging controls).

2. Controls: the compliance components

Objective: build the system that ensures compliance with privacy principles.

Step	Description	Report
	2. Controls 2.1. Legal controls 2.2. Risk-treatment controls *Purpose, information, subjects' rights, etc.* *Actions on personal data, impacts, sources, supporting assets, etc.*	❑ List of selected controls ❑ Detailed description of the controls

Tips for carrying out the actions

- These controls may be created from scratch or taken from good practices issued by recognized institutions or international standards and adapted to the specific context.
- Moreover, any incidents that may have already occurred as well as any difficulties in implementing certain controls may be used to improve the compliance components.
- To improve the reliability of the controls, it is worthwhile to determine the actions planned in case these controls prove to be ineffective (if they no longer work).
- This step is revised until compliance with legal requirements and the risk treatment is sufficient.

2.1. Legal controls (mandatory)

- Identify or determine the **controls** (existing or planned) **selected to comply with the following legal requirements** (it is necessary to explain how it is intended to implement them):
  1. **purpose**: specified, explicit and legitimate purpose[21];
  2. **minimization**: limiting the amount of personal data to what is strictly necessary[22];
  3. **quality**: preserving the quality of personal data[23];
  4. **retention periods**: period needed to achieve the purposes, in the absence of another legal obligation imposing a longer retention period[24];
  5. **information**: respect for data subjects' right to information[25];
  6. **consent**: obtaining the consent of the data subjects or existence of another legal basis justifying the processing of personal data[26];

[21] "*the data shall be obtained for specified, explicit and legitimate purposes*" (Article 6 of [DP-Act] and of [Directive-95-46]).

[22] "*they shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing*" (Article 6 of [DP-Act] and of [Directive-95-46]).

[23] "*they shall be accurate, complete and, where necessary, kept up-to-date*" (Article 6 of [DP-Act] and of [Directive-95-46]). The quality requirement also concerns the relationship between the data that identifies individuals and the data pertaining to them.

[24] "*they shall be retained […] for a period no longer than is necessary for the purposes for which they are obtained and processed*" (see Article 6 of [DP-Act] and of [Directive-95-46]), in the absence of another legal obligation imposing a longer retention period.

[25] See Article 32 of [DP-Act] and Articles 10 and 11 of [Directive-95-46].

7. **right to object**: respect for the data subjects' right of opposition[27];
8. **right of access**: respect for the data subjects' right to access their data[28];
9. **right to rectification**: respect for the data subjects' right to correct their data and erase them[29];
10. **transfers**: compliance with obligations relating to transfer of data outside the European Union[30];
11. **prior checking**: definition and fulfillment of formalities prior to processing.

2.2. Risk-treatment controls

❑ Identify or determine the **selected controls** (existing or planned):

1. **organizational controls**: organization, policy, risk management, project management, incident management, supervision, etc.
2. **logical security controls**: anonymization, encryption, backups, data partitioning, logical access control, etc.
3. **physical security controls**: physical access control, security of hardware, protection against non-human risk sources, etc.

Tips for carrying out the actions

❑ To treat the risks, it is effective to determine the controls in the following order:

1. first **on the governance** of privacy protection: cross-organizational controls to manage and control the protection of privacy (organization, policy, risk management, project management, etc.);
2. then **on the personal data**: controls designed to prevent security breaches (keeping personal data to a minimum, anonymization of personal data, etc.);
3. then, if the above is insufficient to reduce risk to an acceptable level, **on the potential impacts**: controls designed to prevent the consequences of risks from occurring, to identify and limit their effects or to curb them (backups, integrity checks, management of personal data breaches, etc.);
4. then, if the above is insufficient, **on the risk sources**: controls designed to prevent risk sources from acting, to identify and limit their impact or to turn against them (physical and logical access control, encryption, logging, management of third parties, protection against malicious codes, etc.);
5. finally, if the above is insufficient, **on the supporting assets**: controls designed to prevent the exploitation of vulnerabilities, or to detect and limit threats that do occur (operation of the system, monitor, protect the channels, reduce the vulnerabilities of software, hardware, paper documents, etc.).

[26] If necessary, see Article 7 of [DP-Act].

[27] See Article 38 of [DP-Act] and Article 14 of [Directive-95-46].

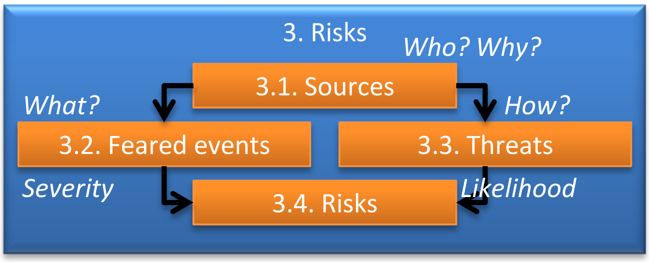
[28] See Article 39 of [DP-Act] and Article 12 of [Directive-95-46].

[29] The data subject may ask that "*data that is inaccurate, incomplete, ambiguous, out-of-date*" or whose "*collection, use, disclosure or retention is prohibited*" should be deleted (see Article 40 of [DP-Act] and Article 12 of [Directive-95-46]).

[30] See Articles 68 and 69 of [DP-Act] and Articles 25 and 26 of [Directive-95-46].

3. Risks: potential privacy breaches

Objective: gain a good understanding of the causes and consequences of risks.

Step	Description	Report
	 3. Risks Who? Why? 3.1. Sources What? How? 3.2. Feared events 3.3. Threats Severity 3.4. Risks Likelihood	❑ Risk map ❑ Detailed description of the risks

3.1. Risk sources

- ❑ Identify the relevant **risk sources** in the specific context under consideration[31].
- ❑ Describe the **capabilities** of risk sources.

3.2. Feared events

- ❑ For each feared event (illegitimate access to personal data[32], unwanted change of personal data[33], and disappearance of personal data[34]):
  - ○ determine the potential **impacts** on the data subjects' privacy if it occurred[35];
  - ○ estimate its **severity**, depending especially on the prejudicial effect of the potential impacts and, if applicable, controls likely to modify them;
  - ○ formally set out a **justification** of the estimation in view of the factors identified.

Examples of feared events

- Data on the habits of employees are illegally collected without the knowledge of the data subjects and used by their superiors to direct research of evidence to fire them (e.g. video surveillance).

- Contact details are retrieved and used without individuals' knowledge for commercial purposes (spam, targeted advertising, etc.).

- Identities are spoofed to perform illegal activities on behalf of data subjects, the latter facing criminal prosecution.

- Following an unwanted modification of health data, patients are inadequately taken care of, thus worsening their condition and even causing disability or death.

- Applications for social benefits vanish, thus depriving the beneficiaries of the said benefits and forcing them to repeat their administrative formalities.

[31] Answer the question "Who or what could be the source of risks that might affect the specific context of the processing(s) of personal data under consideration?".

[32] They are known to unauthorized persons (breach of personal data confidentiality).

[33] They are altered or changed (breach of personal data integrity).

[34] They are not or no longer available (breach of personal data availability).

[35] Answer the question "What do we fear that might happen to data subjects?".

Tips for carrying out the actions

- ❑ It is worthwhile to differentiate existing or planned controls from additional controls, and initial severity from residual severity (which remains, even after these additional controls have been implemented).
- ❑ The impact analysis can also be an opportunity to determine the security needs (expected confidentiality, integrity and availability) useful in the development of a set of specifications.

3.3. Threats

- ❑ Identify **threats** to personal data supporting assets that could lead to each feared event[36].
- ❑ For each identified threat:
    - select the **risk sources** that could cause it;
    - estimate its **likelihood**, particularly depending on the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them;
    - formally set out a **justification** of the estimation in view of the factors identified.

Examples of threats

- A malicious attacker injects unexpected queries into the form on a website.
- A competitor, visiting incognito, steals a portable hard drive.
- A staff member deletes tables from a database by mistake.
- Water damage destroys the computer servers and telecommunications.

Tips for carrying out the actions

- ❑ Identifying threats consists of determining all that can happen to the personal data supporting assets for the feared events to occur; this can be done either empirically (e.g. brainstorming) or systematically (e.g. studying all possible actions on each personal data supporting asset: it could be observed, used in a manner other than planned, altered, deteriorated or destroyed, lost or stolen).
- ❑ Although this is not recommended, it is possible not to study the threats that could allow the occurrence of feared events with negligible or limited severity, or to study only the threats deemed as most likely.

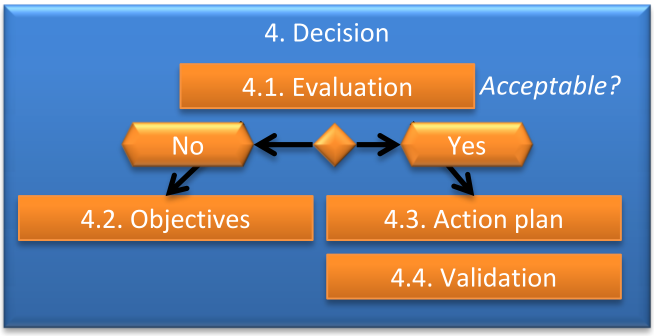
3.4. Risks

- ❑ Determine the risk level[37]:
    - its **severity** equals to that of the feared event concerned by the risk;
    - its **likelihood** equals the highest likelihood value of the threats associated with the feared event.
- ❑ Present a map of all the risks depending on their level.

[36] Answer the question “How can it happen?”.
[37] A risk consists of a feared event and all the threats that may allow it to occur.

4. Decision: validation of the PIA

Objective: decide whether to accept or not the manner in which the PIA was managed and the residual risks[38].

Step	Description	Report
	 4. Decision 4.1. Evaluation Acceptable? No Yes 4.2. Objectives 4.3. Action plan 4.4. Validation	❑ Rationale to validate the PIA ❑ If applicable, action plan(s)

4.1. Evaluation of the PIA

- ❑ Review the results of the preceding steps:
  - ○ check that it is not useful, or not possible, to improve the manner in which each legal control is implemented;
  - ○ check that it is not useful, or not possible, to improve the manner in which each risk is treated;
- ❑ Determine whether or not they are acceptable, with justifications, particularly with regard to previously identified stakes.

4.2. Case 1 – The PIA is not yet deemed acceptable: objectives

- ❑ Determine the **objectives** for legal requirements and risks for which the manner of treating them was not deemed acceptable.
- ❑ Repeat the previous steps.

4.3. Case 2 – The PIA is deemed acceptable: action plan

- ❑ If necessary, prepare an **action plan** for all the planned controls.

Tips for carrying out the actions

- ❑ The controls specified in the action plan should be set out formally, implemented, monitored regularly and improved continuously.

4.4. Case 2 – The PIA is deemed acceptable: formal validation

- ❑ Formally validate the PIA[39].

[38] Risks that remain after the controls have been implemented.

[39] The decision in no manner prejudges the conformity assessment that may be made, if necessary, by the data protection authority (the CNIL in France), for example through prior checking or controls.

Appendix - References used

Acronyms

CISO	Chief Information Security Officer
CNIL	*Commission Nationale de l'Informatique et des Libertés* (the French Data Protection Authority)
DPO	Data Protection Officer
EBIOS	*Expression des Besoins et Identification des Objectifs de Sécurité* – Expression of Needs and Identification of Security Objectives
IS	Information Security

Definitions

Personal data 'Personal data' means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to that person. In order to determine whether a person is identifiable, all the means that the data controller or any other person can use or may have access to should be taken into consideration. [DP-Act]

Feared event Breach of personal data security likely to have impacts on data subjects' privacy.

Risk management Iterative process that allows to objectively manage the privacy risks on the data subjects concerned by a processing of personal data. It essentially consists in appreciating them (identification, estimation in terms of severity and likelihood, and evaluation for comparison), treating them (determining and implementing proportionate controls), accepting residual risks, communicating (stakeholder consultation, results presentation, etc.), and monitoring changes over time (in context, risks, controls, etc.).

Severity Estimation of the magnitude of potential impacts on the data subjects' privacy. It essentially depends on the prejudicial effect of the potential impacts.

Threat Typical action used intentionally or not by risk sources that may cause a feared event.

Control Action to be taken to treat risks. It could be to avoid, reduce, transfer or retain them.

Data subject The 'data subject' of a processing of personal data means an individual to whom the data covered by the processing relate. [DP-Act]

Data controller The ‘data controller’ means, unless expressly designated by legislative or regulatory provisions relating to this processing, a person, public authority, department or any other organization who determines the purposes and means of the data processing. [DP-Act]

Risk Scenario describing a feared event and all threats that make it possible. It is estimated in terms of severity and likelihood.

Risk source Person or non-human source that can cause a risk, accidentally or deliberately.

Supporting asset Asset on which some personal data rely. It can be hardware, software, networks, people, paper or paper transmission channels.

Processing of personal data ‘Processing of personal data’ means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other way of making available, alignment or combination, locking, deletion or destruction. [DP-Act]

Likelihood Estimation of the possibility for a risk to occur. It essentially depends on the level of exploitable vulnerabilities and on the level of capabilities of the risk sources to exploit them.

Vulnerability Characteristic of a personal data supporting asset, that can be used by risk sources and allow threats to occur.

References

[EUCharter] Charter of Fundamental Rights of the European Union, 2010/C 83/02.

[Directive-1995-46] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[Ordinance-2011-1012] Ordinance 2011-1012 on electronic communications transposing particularly Directive 2009/136/EC introducing the obligation of notification of breaches of personal data collected as part of the processing implemented by providers of telecommunications services open to the public.

[DP-Act] Act no. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties as amended[40].

[ISO31000] ISO 31000:2009, Risk management -- Principles and guidelines, ISO.

[PIA-1-Methodology] Guide "*PIA – Methodology*" (procedure for conducting a PIA), CNIL.

[PIA-2-Tools] Guide "*PIA – Tools*" (models and knowledge bases), CNIL.

[PIA-3-GoodPractices] Guide *"PIA – Good practices"* (controls for treating risks), CNIL.

[SecurityGuide] Guide *"Security of Personal Data"*, CNIL.

[EBIOS] Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Expression of needs and identification of security objectives, risk management methodology, January 25, 2010, ANSSI.

[40] Amended by French Act No. 2004-801 of August 6, 2004, on the protection of individuals in regard to the processing of personal data, and by French Act No. 2009-526 of May 12, 2009, on the simplification and clarification of French law and the facilitation of procedures.