PRIVACY IMPACT ASSESSMENT (PIA)

Tools (templates and knowledge bases)

CNIL
Commission Nationale de l'Informatique et des Libertés

June 2015 Edition

Contents

Note: These templates and knowledge bases may have to be adapted.

Foreword

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

- [PIA-1-Methodology], which presents the methodology used to conduct PIAs;
- [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);
- wording in brackets ([text]) correspond to references.

Note: the templates and knowledge bases presented in this guide help implement the approach. It is absolutely possible and even desirable to adapt them to each specific context.

Reminder: 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.

Note: These templates and knowledge bases may have to be adapted.

1. Tools for context study

1.1. General description

Template: General description

The following template can be used to describe the processing in a summarized manner:

Description of the processing	
Purposes of the processing	❑
Stakes of the processing	❑
Data controller	
Processors	❑

Note: These templates and knowledge bases may have to be adapted.

1.2. Detailed description

Template: Description of personal data

The following template can be used to present the personal data:

Personal data	Categories	Personal data recipients (and justifications)	People with access to them (and justifications)	Retention period (and justifications)

Notes

- Personal data are generally considered as a whole in the rest of the study.
- However, their description should be detailed in this section. Depending on the size and complexity of the personal data processing(s) under consideration, but also depending on what we wish to highlight, personal data can be grouped into consistent and easy-to-study sets.

Knowledge base: Typology of personal data

Personal data categories are generally as follows:

Personal data types	Personal data categories
Common personal data	Civil status, identity, identification data
	Personal life (living habits, marital status, etc. –excluding sensitive or dangerous data)
	Professional life (résumé, education and professional training, awards, etc.)
	Economic and financial information (income, financial situation, tax situation, etc.)
	Connection data (IP addresses, event logs, etc.)
	Location data (travels, GPS data, GSM data, etc.)
Personal data perceived as sensitive	Social security number
	Biometric data
	Bank data
Sensitive personal data in the meaning of [DP-Act][1]	Philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, data concerning health or sex life
	Offenses, convictions, security measures

[1] See Articles 8 and 9 of [DP-Act] and Article 8 of [Directive-95-46].

Note: These templates and knowledge bases may have to be adapted.

Template: Description of personal data supporting assets

The following template can be used to present personal data supporting assets for each process in the personal data processing operation(s) considered:

Generic processes	Detailed description of the process	Information systems[2] on which personal data rely	Other supporting assets[3] on which personal data rely
Collection			
Retention			
Use			
Transfer			
Destruction			

Notes

- The process of "use" generally needs to be broken down into as many processes as used by the processing.
- Personal data supporting assets can be grouped into consistent sets.

Knowledge base: Typology of personal data supporting assets

Personal data supporting assets are components of the information system on which personal data rely:

Types of personal data supporting assets		Examples
Information systems	Hardware and electronic data media	Computers, communications relays, USB drives, hard drives
	Software	Operating systems, messaging, databases, business applications
	Computer channels	Cables, WiFi, fiber optic
Organizations	People	Users, IT administrators, policymakers
	Paper documents	Prints, photocopies, handwritten documents
	Paper transmission channels	Mail, workflow

Notes

- It is necessary to choose the most appropriate level of detail for the study.
- Security solutions (products, procedures, controls, etc.) are not personal data supporting assets: these are controls intended to treat the risks.

[2] Can be broken down into hardware (and electronic data media), software and computer channels.
[3] Can be broken down into people, paper documents and paper transmission channels.

Note: These templates and knowledge bases may have to be adapted.

2. Tools for controls study

2.1. Legal controls (mandatory)

Template: Compliance system to meet legal requirements

The following template can be used to present existing or planned controls:

Themes	Check points	Main effect	Description of controls / Justifications
1. Legal controls (mandatory)	Purpose: specified, explicit and legitimate purpose[4]	Data	
	Minimization: limiting the amount of personal data to what is strictly necessary[5]	Data	
	Quality: preserving the quality of personal data[6]	Data	
	Retention periods: period needed in order to achieve the purposes, in the absence of another legal obligation imposing a longer retention period[7]	Data	
	Information: respect for data subjects' right to information[8]	Data	
	Consent: obtaining the consent of data subjects or existence of another legal basis justifying the processing of personal data [9]	Data	
	right to object: respect for the data subjects' right to object[10]	Data	
	Right of access: respect for data subjects' right to access their data[11]	Data	
	Right to rectification: respect for data subjects' right to correct their data and erase them[12]	Data	

[4] "*the data shall be obtained for specified, explicit and legitimate purposes*" (Article 6 of [DP-Act] and of [Directive-95-46]).
[5] "*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]).
[6] "*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.
[7] "*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.
[8] See Article 32 of [DP-Act] and Articles 10 and 11 of [Directive-95-46].
[9] If necessary, see Article 7 of [DP-Act].
[10] See Article 38 of [DP-Act] and Article 14 of [Directive-95-46].
[11] See Article 39 of [DP-Act] and Article 12 of [Directive-95-46].

Note: These templates and knowledge bases may have to be adapted.

Themes	Check points	Main effect	Description of controls / Justifications
	Transfers: compliance with obligations relating to transfer of data outside the European Union[13]	Data	
	Priori checking: definition and fulfillment of formalities prior to processing	Data	

2.2. Risk-treatment controls

Template: Compliance system to treat risks

The following template can be used to present existing or planned controls:

Themes	Check points	Main effect	Description of controls / Justifications
2. Organizational controls	Organization	Cross-organizational	
	Policy (management of rules)	Cross-organizational	
	Risk management	Cross-organizational	
	Project management	Cross-organizational	
	Management of incidents and data breaches	Impacts	
	Staff management	Sources	
	Relationships with third parties	Sources	
	Maintenance	Sources	
	Supervision (audits, dashboards, etc.)	Cross-organizational	
	Marking of documents	Sources	
	Archival	Cross-organizational	
3. Logical security controls	Anonymization	Data	
	Encryption	Sources	
	Integrity checks	Impacts	
	Backups	Impacts	
	Data partitioning	Sources	
	Logical access control	Sources	
	Traceability	Sources	
	Operations	Supporting assets	
	Monitoring (settings, configuration controls, real-time monitoring, etc.)	Supporting assets	
	Workstation management	Supporting assets	

[12] 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]).

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

Note: These templates and knowledge bases may have to be adapted.

Themes	Check points	Main effect	Description of controls / Justifications
	Fight against malicious code (viruses, spyware, software bomb, etc.)	Sources	
	Protection of computer channels (networks)	Supporting assets	
4. Physical security controls	Distancing of risk sources (dangerous products, dangerous geographic areas, etc.)	Sources	
	Physical access control	Sources	
	Security of hardware	Supporting assets	
	Security of paper documents	Supporting assets	
	Security of paper channels	Supporting assets	
	Protection from non-human risk sources (fire, water, etc.)	Sources	

Note: These templates and knowledge bases may have to be adapted.

3. Tools for risks study

3.1. Risk sources

Template: Study of risks sources

The following template can be used to present the selected risk sources:

Types of risk sources	Relevant risk sources	Description of capabilities[14]
Internal human sources acting accidentally		
Internal human sources acting deliberately		
External human resources acting accidentally		
External human sources acting deliberately		
Internal non-human sources		
External non-human sources		

Notes

- If several risk sources are identified for a given type, then the one that has the greatest capability must be taken into account in the study of risks.

Knowledge base: Typology of risk sources

The following table shows examples of risk sources:

Types of risk sources	Examples
Internal human sources	Employees, IT managers, trainees, managers
External human sources	Recipients of personal data, authorized third parties[15], service providers, hackers, visitors, former employees, activists, competitors, customers, maintenance staff, maintenance, offenders, trade unions, journalists, non-governmental organizations, criminal organizations, organizations under the control of a foreign state, terrorist organizations, nearby industrial activities
Non-human sources	Malicious code of unknown origin (viruses, worms, etc.), water (pipelines, waterways, etc.), flammable, corrosive or explosive materials, natural disasters, epidemics, animals

[14] Their capabilities include their proximity to personal data supporting assets, skills, financial resources, time available, etc. and, in the case of human sources, the reasons for their action in accidental cases (blunder, thoughtlessness, poor understanding of commitment, lack of motivation in one's relationship with the organization, etc.) or their motivation in deliberate cases (game, ego, revenge, profit motive, feeling of impunity, etc.).

[15] For example, public authorities and court officers may request disclosure of certain data when the law expressly permits them to do so.

Note: These templates and knowledge bases may have to be adapted.

3.2. Feared events

Template: Study of feared events

The following template can be used to present the feared events:

Potential data breaches	Risk sources	Outcomes / objectives pursued	Potential impacts	Controls	Severity	Justification
Illegitimate access to personal data		❑ None ❑ Storage ❑ Redistribution ❑ Correlation ❑ Use ❑ Other (specify)				
Unwanted modification of personal data		❑ Malfunction ❑ Use ❑ Other (specify)				
Disappearance of personal data		❑ Malfunction ❑ Blockage ❑ Other (specify)				

Notes

- The wording of the three feared events, studied systematically in a PIA, can be adapted so that it is better understood by stakeholders.
- The risk sources are those deemed relevant in the context considered, to be the source of the feared event.
- The outcomes / objectives pursued are the outcome(s) of the feared event(s) deemed relevant in the context considered.
- The potential impacts are the list of possible consequences for the privacy of data subjects.
- Risk sources are relevant sources to be the cause of each feared event in the context considered.
- The controls are, where appropriate, the list of existing or planned controls that affect the severity of the feared event considered.
- Severity is estimated using the chosen scales and calculation rules.
- The justification explains how the severity has been determined (for example, for a "limited" severity in a given context: "The personal data are perfectly identifiable and the potential impacts are significant, but the controls can greatly reduce the prejudicial effect").
- When we divide personal data into several subsets (when we do not consider them as a whole), the feared events are multiplied into as many subsets.
- If it appears that the impacts differ significantly depending on the risk sources (i.e. internal or external illegitimate access, accident or attack, etc.) or the outcomes of a feared event (e.g. alteration into data that no longer have meaning or into other valid

Note: These templates and knowledge bases may have to be adapted.

personal data, temporary or permanent disappearance, etc.), it may also be relevant to break down the feared events.

- To clearly distinguish the impacts on the privacy of data subjects from the impacts on the organization (e.g. image loss, financial loss, business disruption, legal consequence, etc.), it may be useful to identify and present these two types of impacts; but in this case, only the first will be used to estimate the severity of the feared events in a PIA.

Knowledge base: Typology of the outcomes of feared events

Feared events may have different consequences if they occur:

Feared events	Types of outcomes	Description
Illegitimate access to personal data	None	The data are seen by people who do not need to know them, though these people do not use them.
	Storage	The data are copied and saved to another location without being further used.
	Redistribution	The data are disseminated more than necessary and beyond the control of the data subjects (e.g. unwanted dissemination of a photo on the Internet, loss of control over information published in a social network, etc.)
	Use	The data are used for purposes other than those planned and/or in an unfair manner (e.g. commercial purposes, identity theft, use against data subjects, etc.) or correlated with other information relating to the data subjects (e.g. correlation of residence address and real-time geolocation data, etc.)
Unwanted modification of personal data	Malfunction	The data are modified into valid or invalid data, which will not be used correctly, the processing liable to cause errors, malfunctions, or no longer provide the expected service (e.g. impairing the proper progress of important steps, etc.)
	Use	The data are modified in other valid data, such that the processing operations have been or could be misused (e.g. use to steal identities by changing the relationship between the identity of individuals and the biometric data of other individuals, etc.).
Disappearance of personal data	Malfunction	The data are missing for personal data processings, which generates errors, malfunctions, or provides a different service than the one expected (e.g. some allergies are no longer reported in a medical record, some information contained in tax returns has disappeared, which prevents the calculation of the tax amount, etc.)
	Blockage	The data are missing for personal data processings which can no longer provide the expected service (e.g. slowing down or blocking of administrative or commercial processes, inability to provide care due to the loss of medical records, inability of data subjects to exercise their rights, etc.).

Note: These templates and knowledge bases may have to be adapted.

Knowledge base: Scales and rules for estimating risks

The following elements may be used to estimate severity and likelihood.

Notes

- Risk assessment can be performed in various ways, provided that one severity and one likelihood are obtained for each risk.
- Risk assessment is necessarily subjective, but this subjectivity is counterbalanced by clear scales and rules and an estimation that is based on the consensus of the stakeholders.
- The scales and rules used are important communication elements, which must be understood, accepted and usable by stakeholders.

Scales and rules for estimating severity

Severity represents the magnitude of a risk. It is primarily estimated in terms of the extent of potential impacts on data subjects, taking account of existing, planned or additional controls (which should be mentioned as justification).

The following scale can be used to estimate the severity of feared events (**Important: these are only examples, which can be very different depending on the context**):

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[16]	Examples of material impacts[17]	Examples of moral impacts[18]
1. Negligible	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem	- Lack of adequate care for a dependent person (minor, person under guardianship) - Transient headaches	- Loss of time in repeating formalities or waiting for them to be fulfilled - Receipt of unsolicited mail (e.g. spams) - Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing) - Targeted advertising for common consumer products	- Mere annoyance caused by information received or requested - Fear of losing control over one's data - Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion) - Loss of time in configuring one's data - Lack of respect for the freedom of online movement due to the denial of access to a commercial site (e.g. alcohol because of the wrong age)
2. Limited	Data subjects may encounter significant inconveniences, which they will be able to	- Minor physical ailments (e.g. minor illness due to disregard of	- Unanticipated payments (e.g. fines imposed erroneously), additional costs (e.g. bank charges, legal fees), payment defaults	- Refusal to continue using information systems (whistleblowing, social

[16] Loss of amenity, disfigurement, or economic loss related to physical integrity.
[17] Loss incurred or lost revenue with respect to an individual's assets.
[18] Physical or emotional suffering, disfigurement or loss of amenity.

Note: These templates and knowledge bases may have to be adapted.

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[16]	Examples of material impacts[17]	Examples of moral impacts[18]
	overcome despite a few difficulties	contraindications) - Lack of care leading to a minor but real harm (e.g. disability) - Defamation resulting in physical or psychological retaliation	- Denial of access to administrative services or commercial services - Lost opportunities of comfort (i.e. cancellation of leisure, purchases, holiday, termination of an online account) - Missed career promotion - Blocked online services account (e.g. games, administration) - Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects - Cost rise (e.g. increased insurance prices) - Non-updated data (e.g. position held previously) - Processing of incorrect data creating for example accounts malfunctions (bank, customers, with social organizations, etc.) - Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g. pregnancy advertising, drug treatment) - Inaccurate or inappropriate profiling	networks) - Minor but objective psychological ailments (defamation, reputation) - Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation, loss of recognition) - Feeling of invasion of privacy without irreversible damage - Intimidation on social networks
3. Significant	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	- Serious physical ailments causing long-term harm (e.g. worsening of health due to improper care, or disregard of contraindications) - Alteration of physical integrity for example following an assault, an accident at home, work, etc.	- Misappropriation of money not compensated - Non-temporary financial difficulties (e.g. obligation to take a loan) - Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban) - Prohibition on the holding of bank accounts - Damage to property - Loss of housing - Loss of employment - Separation or divorce - Financial loss as a result of a fraud (e.g. after an attempted phishing) - Blocked abroad - Loss of customer data	- Serious psychological ailments (e.g. depression, development of a phobia) - Feeling of invasion of privacy with irreversible damage - Feeling of vulnerability after a summons to court - Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression) - Victim of blackmailing - Cyberbullying and harassment
4. Maximum	Data subjects may encounter significant, or even irreversible, consequences, which they may not	- Long-term or permanent physical ailments (e.g. due to disregard of	- Financial risk - Substantial debts - Inability to work - Inability to relocate - Loss of evidence in the context of	- Long-term or permanent psychological ailments - Criminal penalty - Abduction

Note: These templates and knowledge bases may have to be adapted.

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[16]	Examples of material impacts[17]	Examples of moral impacts[18]
	overcome	contraindications) - Death (e.g. murder, suicide, fatal accident) - Permanent impairment of physical integrity	litigation - Loss of access to vital infrastructure (water, electricity)	- Loss of family ties - Inability to sue - Change of administrative status and/or loss of legal autonomy (guardianship)

The value of the level that best matches the potential impacts identified is then selected, by comparing the impacts identified in the context considered with the generic impacts in the scale.

The severity level thus obtained may be raised or lowered by including additional factors:

- level of identification of personal data;
- nature of risk sources;
- number of interconnections (especially with foreign sites);
- number of recipients (which facilitates the correlation between originally separated personal data).

Note: These templates and knowledge bases may have to be adapted.

Scale and rules for estimating likelihood

Likelihood represents the feasibility of a risk to occur. It is primarily estimated in terms of the level of vulnerabilities of the supporting assets concerned and the level of capabilities of the risk sources to exploit them, taking account of existing, planned or additional controls (which should be mentioned as justification).

The following scale can be used to estimate the likelihood of threats:

1. Negligible: it does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
2. Limited: it seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in a room protected by a badge reader).
3. Significant: it seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).
4. Maximum: it seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in the public lobby).

The value of the level that best matches the vulnerabilities of the supporting assets and the risk sources is then selected.

The likelihood level thus obtained may be raised or lowered by including additional factors:

- opening on the Internet or a closed system;
- data exchanges with foreign countries or not;
- interconnections with other systems or no interconnection;
- heterogeneity or homogeneity of the system;
- variability or stability of the system;
- the organization's image.

Note: These templates and knowledge bases may have to be adapted.

3.3. Threats

Template: Study of threats

The following template can be used to present the threats:

Threats	Risk sources	Controls	Likelihood	Justification

Notes

- The wording of the threats derived from the knowledge bases presented below can be adapted so that it is better understood by the stakeholders or reflect the threats more explicitly.
- If some threats are not applicable (e.g. threats relating to paper documents in a context where there are no paper documents), it is then preferable to leave them in the table and explain it in the justification.
- Risk sources are relevant sources to be the origin of each threat in the context considered.
- The controls are, where appropriate, the list of existing or planned controls that affect the likelihood of the threat considered.
- Likelihood is estimated using the selected scales and calculation rules.
- The justification explains how the likelihood level has been determined (for example, for a "negligible" likelihood in a given context: "the vulnerabilities of supporting assets are significant and the capabilities of the risk sources to exploit them are maximum, but the controls can reduce them greatly").

Knowledge base: Typology of threats

The action of risk sources on the supporting assets constitutes a threat and can take the form of different threats. The supporting assets can be:

- used inappropriately: supporting assets are used outside or even diverted from their intended context of use without being altered or damaged;
- observed: supporting assets are observed or spied upon without being damaged;
- overloaded: the limits of operation of supporting assets are exceeded, supporting assets are overloaded, over-exploited or used under conditions not permitting them to function properly;
- damaged: supporting assets are partially or completely damaged;
- altered: supporting assets are transformed;
- lost: supporting assets are lost, stolen, sold or given away, so it is no longer possible to exercise property rights.

Note: These templates and knowledge bases may have to be adapted.

The generic threats that follow are designed to be exhaustive, independent and applied to the specific features of privacy protection.

Threats that can lead to an illegitimate access to personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
C	Hardware	Used inappropriately	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, the hard drive containing the information is used for purposes other than the intended purpose (e.g. to transport other data to a service provider, to transfer other data from one database to another, etc.)	Usable for other than the intended purpose, disproportion between hardware capacities and the required capacities (e.g. hard drive of several TB to store few GB of data)
C	Hardware	Observed	Watching a person's screen without their knowledge while on the train; taking a photo of a screen; geolocation of hardware; remote detection of electromagnetic signals	Allows interpretable data to be observed; generates compromising emanations
C	Hardware	Altered	Tracking by a hardware-based keylogger; removal of hardware components; connection of devices (such as USB flash drives) to launch an operating system or retrieve data	Allows components (boards, expansion cards) to be added, removed or substituted via connectors (ports, slots); allows components to be disabled (USB port)
C	Hardware	Lost	Theft of a laptop from a hotel room; theft of a work cell phone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device	Small, appealing targets (market value)
C	Software	Used inappropriately	Content scanning; illegitimate cross-referencing of data; raising of privileges, erasure of tracks; sending of spam via an e-mail program; misuse of network functions	Makes data accessible for viewing or manipulation (deletion, modification, movement); may be used for other than normal purposes; allows the use of advanced functionalities
C	Software	Observed	Scanning of network addresses and ports; collection of configuration data; analysis of source codes in order to locate exploitable flaws; testing of how databases respond to malicious queries	Possibility of observing the functioning of software; access to and reading of source codes
C	Software	Altered	Tracking by a software-based key logger; infection by malicious code; installation of a remote administration tool; substitution of components during an update, a maintenance operation or installation (code-bits or applications are installed or replaced)	Editable (improvable, configurable); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources); does not function properly or as expected
C	Computer channels	Observed	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network	Permeable (generation of compromising emanations); allows interpretable data to be observed
C	People	Observed	Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings	People who cannot keep things to themselves, are predictable (with routine lives that make repeated espionage easy)
C	People	Manipulated	Influence (phishing, social engineering, bribery), pressure (blackmail, psychological harassment)	Easily influenced (naive, gullible, obtuse, low self-esteem, little loyalty), easily manipulated (vulnerable to pressure placed on themselves or their circle of family and friends)
C	People	Lost	Employee poaching; assignment changes; takeover of all or part of the organization	Little loyalty to the organization; personal needs that are largely unmet; easy breach of contractual obligations

Note: These templates and knowledge bases may have to be adapted.

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
C	Paper documents	Observed	Reading, photocopying, photographing	Allows interpretable data to be seen
C	Paper documents	Lost	Theft of files from offices; theft of mail from mailboxes; retrieval of discarded documents	Portable
C	Paper transmission channels	Observed	Reading of signature books in circulation; reproduction of documents in transit	Observable

Threats that can lead to an unwanted modification of personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
I	Hardware	Altered	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of an application	Allows components (boards, expansion cards) to be added, removed or substituted via connectors (ports, slots); allows components to be disabled (USB port)
I	Software	Used inappropriately	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data	Makes data accessible for viewing or manipulation (deletion, modification, movement); may be used for other than normal purposes; allows the use of advanced functionalities
I	Software	Altered	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components	Editable (improvable, configurable); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources); does not function properly or as expected
I	Computer channels	Used inappropriately	Man-in-the-middle attack to modify or add data to network traffic; replay attack (resending of intercepted data)	Allows traffic to be altered (interception then resending of data, possibly altered); sole means of transmission for the flow; allows the computer channel-sharing rules to be changed (transmission protocol authorizing the addition of nodes)
I	People	Overloaded	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills	Insufficient resources for assigned tasks; capacities not suited to working conditions; insufficient skills for carrying out duties Inability to adapt to change
I	People	Manipulated	Influence (rumor, disinformation)	Easily influenced (naive, gullible, obtuse)
I	Paper documents	Altered	Changes to figures in a file; replacement of an original by a forgery	Falsifiable (paper documents with editable content)
I	Paper transmission channels	Altered	Changes to a memo without the author's knowledge; change from one signature book to another; sending of multiple conflicting documents	Allows distributed documents to be altered; sole means of transmission for the channel; allows the paper transmission channel to be altered

Note: These templates and knowledge bases may have to be adapted.

Threats that can lead to a disappearance of personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
D	Hardware	Used inappropriately	Storage of personal files; personal use	Usable for purposes other than the intended purpose
D	Hardware	Overloaded	Storage unit full; power outage; processing capacity overload; overheating; excessive temperatures, denial of service attack	Storage capacities too low; processing capacities too low and not adapted to the processing conditions; constant electricity supply required for operation; sensitive to voltage variations
D	Hardware	Altered	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of the system	Allows components (boards, expansion cards) to be added, removed or substituted via connectors (ports, slots); allows components to be disabled (USB port)
D	Hardware	Damaged	Flooding, fire, vandalism, damage from natural wear and tear, storage device malfunction	Poor-quality components (fragile, easily flammable, poor aging resistance); not suited to the conditions of use; erasable (vulnerable to magnetic fields or vibrations)
D	Hardware	Lost	Theft of a laptop, loss of a cell phone; disposal of a supporting asset or hardware, under-capacity drives leading to a multiplication of supporting assets and to the loss of some	Portable, appealing targets (market value)
D	Software	Used inappropriately	Erasure of data; use of counterfeit or copied software; operator errors that delete data	Makes data accessible for viewing or manipulation (deletion, modification, movement); may be used for other than normal purposes; allows the use of advanced functionalities
D	Software	Overloaded	Exceeding of database size; injection of data outside the normal range of values, denial of service attack	Allows any kind of data to be entered; allows any volume of data to be entered; allows actions to be executed using input data; low interoperability
D	Software	Altered	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components	Editable (improvable, configurable); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources); does not function properly or as expected
D	Software	Damaged	Erasure of a running executable or source codes; logic bomb	Possibility of erasing or deleting programs; sole copy; complex in terms of use (not very user-friendly, few explanations)
D	Software	Lost	Non-renewal of the license for software used to access data, stoppage of security maintenance updates by the publisher, bankruptcy of the publisher, corruption of storage module containing the license numbers	Sole copy (of license agreements or software, developed internally.); appealing (rare, innovative, high commercial value.); transferable (full transfer clause in license)
D	Computer channels	Overloaded	Misuse of bandwidth; unauthorized downloading; loss of Internet connection	Non-scalable transmission capacities (insufficient bandwidth; limited amount of telephone numbers)
D	Computer channels	Damaged	Cut wiring, poor Wi-Fi reception, corrosion of cables	Alterable (fragile, breakable, poor cable structure, bare cables, disproportionate sheath), sole
D	Computer channels	Lost	Theft of copper cables	Appealing targets (market value of cables), transportable (lightweight, may be hidden); inconspicuous (easily forgotten, trivial, do not stand out)

Note: These templates and knowledge bases may have to be adapted.

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
D	People	Overloaded	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills	Insufficient resources for assigned tasks; capacities not suited to working conditions; insufficient skills for carrying out duties; inability to adapt to change
D	People	Damaged	Occupational accident; occupational disease; other injury or disease; death; neurological, psychological or psychiatric ailment	Physical, psychological or mental limits
D	People	Lost	Death, retirement, reassignment; contract termination or dismissal; takeover of all or part of the organization	Little loyalty to the organization; personal needs that are largely unmet; easy breach of contractual obligations
D	Paper documents	Used inappropriately	Gradual erasure over time; voluntary erasure of portions of a document, reuse of paper to take notes not related to the processing, to make a shopping list, use of notebooks for something else	Editable (paper document with erasable content, thermal papers not resistant to temperature changes)
D	Paper documents	Damaged	Aging of archived documents; burning of files during a fire	Poor-quality components (fragile, easily flammable, poor aging resistance); not suited to the conditions of use
D	Paper documents	Lost	Theft of documents; loss of files during a move; disposal	Portable
D	Paper transmission channels	Overloaded	Mail overload; overburdened validation process	Existence of quantitative or qualitative limits
D	Paper transmission channels	Damaged	End of workflow following a reorganization; mail delivery halted by a strike	Unstable, sole
D	Paper transmission channels	Altered	Change in how mail is sent; reassignment of offices or premises; reorganization of paper transmission channels; change in working language	Editable (replaceable)
D	Paper transmission channels	Lost	Elimination of a process following a reorganization; loss of a document delivery company, vacancy	Unrecognized need

Note: These templates and knowledge bases may have to be adapted.

3.4. Risks

Template: Study of risks

The table below can be used to present the risks:

Risks	Examples	Main controls	Main impacts	Severity	Main threats	Likelihood
Illegitimate access to personal data						
Unwanted modification of personal data						
Disappearance of personal data						

A diagram such as the one below can be used to present the risk map:

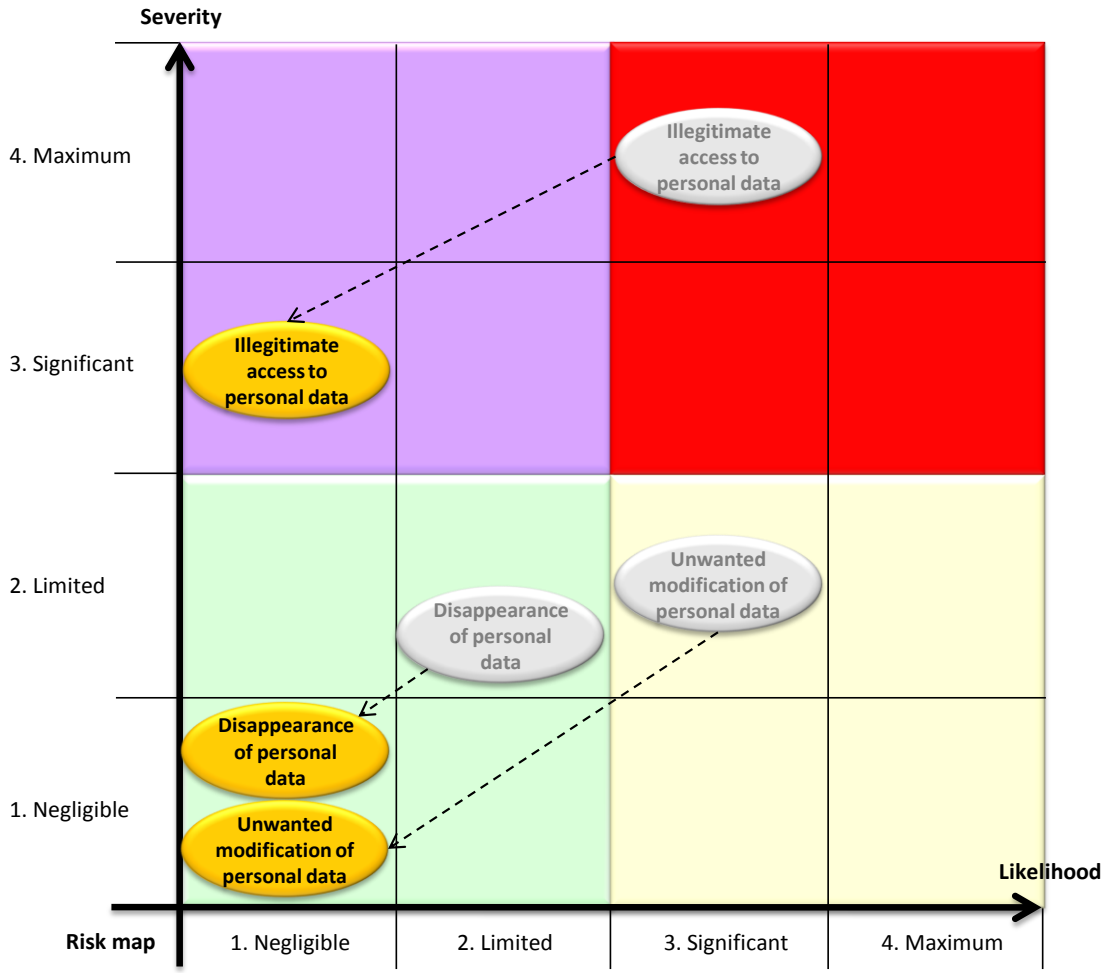

Figure 1 – Risk map

Note: These templates and knowledge bases may have to be adapted.

4. Tools for validating the PIA

4.1. Evaluation of the PIA

Template: Evaluation of legal controls and residual risks

The table below can be used to summarize the evaluation of the PIA:

	Wording	Acceptability (and arguments)
Legal controls	Purpose	
	Minimization	
	Quality	
	Retention periods	
	Information	
	Consent	
	Right to object	
	Right of access	
	Right to rectification	
	Transfers	
	Priori checking	
Risks	Illegitimate access to personal data	
	Unwanted modification of personal data	
	Disappearance of personal data	

Notes

- We can demonstrate both that the risks are well treated and that controls are all useful by creating a table with controls in the rows, risks in the columns and a cross in each cell where a control contributes to the treatment of a risk.
- It is useful to give examples of residual risks to demonstrate that they can be accepted.

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

Template: Identification of objectives

The table below can be used to formulate the objectives:

	Wording	Objective
Legal controls	Purpose	
	Minimization	
	Quality	
	Retention periods	
	Information	
	Consent	
	Right to object	

Note: These templates and knowledge bases may have to be adapted.

	Wording	Objective
	Right of access	
	Right to rectification	
	Transfers	
	Priori checking	
Risks	Illegitimate access to personal data	
	Unwanted modification of personal data	
	Disappearance of personal data	

Knowledge base: Typology of objectives to treat risks

Objectives can be set depending on the risk level, for example:

1. Risks with a high severity and likelihood[19]: these risks must be absolutely avoided or reduced by implementing security controls that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that they are treated by independent controls of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event);

2. Risks with a high severity but a low likelihood[20]: these risks must be avoided or reduced by implementing security controls that reduce both their severity and their likelihood. Emphasis must be placed on preventive controls. These risks can be taken, but only if it is shown that it is not possible to reduce their severity and if their likelihood is negligible;

3. Risks with a low severity but a high likelihood: these risks must be reduced by implementing security controls that reduce their likelihood. Emphasis must be placed on recovery controls. These risks can be taken, but only if it is shown that it is not possible to reduce their likelihood and if their severity is negligible;

4. Risks with a low severity and low likelihood: it should be possible to take these risks, especially since the treatment of other risks should also lead to their treatment.

Notes

- The risks can generally be reduced, transferred or retained. However, some risks cannot be taken, especially when sensitive data are processed or when the damages that data subjects may sustain are very significant. In such cases it may be necessary to avoid them, for example by not implementing all or part of the processing.

[19] Levels 3. Important and 4. Maximum.
[20] Levels 1. Negligible and 2. Limited.

Note: These templates and knowledge bases may have to be adapted.

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

Template: Formalization of the action plan

The table below can be used to develop the action plan and monitor its implementation:

Control	Controller	Difficulty	Financial cost	Term	Progress

Knowledge base: Scales for the action plan

The scales below can be used to develop the action plan and monitor its implementation:

Criteria	Level 1	Level 2	Level 3
Difficulty	Low	Moderate	High
Financial cost	Nil	Moderate	High
Term	Quarter	Year	3 years
Progress	Not started	In progress	Completed

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

Template: Formalization of the validation

The wording below shows a way of carrying out the formal validation of the PIA:

Validation of the PIA	On [date], [identity or function] validates the PIA in the light of the study conducted and the PIA report. The treatment should allow [synthesis of stakes]. The manner in which it is planned to implement the legal requirements and treat the risks is deemed acceptable in view of these stakes. The implementation of the action plan as well as the continuous improvement of the PIA should be demonstrated. [Signature]

Note: These templates and knowledge bases may have to be adapted.