

METHODOLOGY FOR PRIVACY RISK MANAGEMENT

How to implement the Data Protection Act



Édition 2012

Contents

| | |
|--|-----------|
| FOREWORD | 4 |
| INTRODUCTION | 5 |
| 1. THEORY: RISK MANAGEMENT CONCEPTS | 6 |
| 1.1. The notion of privacy risk | 6 |
| Feared events: what has to be avoided | 6 |
| Threats: what we have to protect from | 7 |
| Level of risks: how to estimate them? | 8 |
| 1.2. The privacy risk management approach | 9 |
| 2. PRACTICE: EBIOS IN THE FIELD OF PRIVACY | 10 |
| 2.1. Background study: What is the context? | 10 |
| 2.2. Feared events study: What does one fear happening? | 12 |
| 2.3. Threats study: How can it happen? (if needed) | 15 |
| 2.4. Risk study: What is the risk level? (if needed) | 18 |
| 2.5. Measures study: What can be done to treat risks? | 20 |
| APPENDICES | 24 |
| Generic threats | 24 |
| Threats that may jeopardize confidentiality | 24 |
| Threats that may jeopardize integrity | 25 |
| Threats that may jeopardize availability | 26 |
| Acronyms | 28 |
| Definitions | 28 |
| References | 31 |

Tables

| | |
|---|----|
| TABLE 1 – DETERMINING THE SEVERITY OF EACH FEARED EVENT | 13 |
| TABLE 2 – FEARED EVENTS STUDY | 14 |
| TABLE 3 – DETERMINING THE LIKELIHOOD OF EACH THREAT | 16 |
| TABLE 4 – THREATS STUDY | 17 |
| TABLE 5 – SELECTED RISK-TREATMENT MEASURES | 23 |
| TABLE 6 – THREATS THAT MAY JEOPARDIZE CONFIDENTIALITY | 24 |
| TABLE 7 – THREATS THAT MAY JEOPARDIZE INTEGRITY..... | 25 |
| TABLE 8 – THREATS THAT MAY JEOPARDIZE AVAILABILITY | 27 |

Figures

| | |
|--|----|
| FIGURE 1 – DETERMINATION OF THE LEVEL OF EACH RISK..... | 8 |
| FIGURE 2 – RISK COMPONENTS | 8 |
| FIGURE 3 – THE FIVE ITERATIVE STEPS OF THE APPROACH..... | 9 |
| FIGURE 4 – RISK MAP | 18 |
| FIGURE 5 – RESIDUAL RISK MAP..... | 21 |

METHODOLOGY OF TRANSLATION

As a principle, it was decided not to translate the original titles of French institutions or procedures which appear in the text, when their translation may be misleading.

For example, the title of the “Commission Nationale de l’Informatique et des Libertés” (CNIL), the French Data Protection Authority, was not translated and it appears as such or under its acronym (CNIL) in the body of the text.

It has been decided not to translate the references tag [example] when the referred document was not available in English.

This English version of “Gérer les risques sur les libertés et la vie privée, la méthode” is provided for informative purposes, only as a courtesy for the non-French reading public. While the CNIL has tried to provide an accurate translation of the original guide available in French, in case of discrepancies between the two texts, the French version shall prevail.

Foreword

This document was drawn up by the Expertise Department of the CNIL, with the kind support of several reviewers¹, and presented to different working groups². It describes a method for managing the risks that the processing of personal data can generate to individuals. Following the guide [CNIL-SecPersonalData], this method consists in a complete analytical approach for improving the management of processing of personal data, especially when they are complex or when identified stakes are high. It is linked to a catalog of measures intended to address the risks assessed with this method.

The use of this approach depends on the processing of personal data on which it is applied: it will probably not be very useful for a single file created to monitor the progress of a project, whereas it will be necessary for a complex processing of sensitive personal data.

Applying this method does not replace the formalities that data controllers have to fill in to the CNIL prior to commencing data processing. This is a rational approach that is going to facilitate their work.

This document is primarily intended for use by controllers, and in particular by stakeholders in the creation or improvement of processing of personal data:

- ❑ controllers, who may have to justify to the CNIL on what measures they have chosen to implement in their systems;
- ❑ project owners / business, who have to assess the risks to their systems and set security objectives;
- ❑ prime contractors / operation, who have to propose solutions to treat risks in accordance with the objectives identified by the projects owners;
- ❑ personal data protection officers (DPO), who have to accompany the project owners in the protection of personal data;
- ❑ chief information security officers (CISO), who have to accompany the project owners in the field of information security (IS).

It aims to assist them in law [Act-I&L]³ enforcement and should enable them:

- ❑ to have an rational view of risks arising from their processing of personal data;
- ❑ to know how to determine security measures, necessary and sufficient 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"* ([Act-I & L] Article 34).

Note: the wording in brackets ([text]) corresponds to the references.

¹ Barbara DASKALA (ENISA), Daniel LE METAYER (INRIA) and other anonymous contributors.

² Including Club EBIOS (on risk management) and NETFOCUS (on information security).

³ Resolution No. 81-094 of 21 July 1981 on the adoption of a recommendation relative to general measures for computer system security already stated that the risk assessment and the general security study are systematically performed for any new processing, and reviewed for existing processing.

Introduction

The personal data have to be distinguished from other information within information systems.

They can represent a value to the organization that processes them. But their processing causes also *de facto* significant liability due to the risks brought upon on the privacy⁴ of data subjects. They 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 they have a value for others. This includes a market value if they are exploited for commercial purposes (spam, targeted advertising...), or a nuisance value in the case of unfair actions (discrimination, refusal of access to benefits, dismissal...) or malicious actions (identity theft, defamation, threats, blackmail, burglary, assault...).

Since a controller processes personal data, he has to comply with [\[Act-I&L\]](#).

First, he has to ensure that the purposes of the processing of personal data are defined, that the collected data are relevant to these purposes, and that they are deleted at the end of a determined period.

He also has to ensure that data subjects are informed and can exercise their rights (opposition, access, rectification and deletion). Whether these rights are taken into account at the level of the organization and whether the exercise of these rights is effective, have to be assessed.

In addition, he has to ensure the security of the data he processes. [\[Act-I&L\]](#) states in Article 34 the obligation for any controller 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.*" It is therefore necessary to identify the risks related to the processing of personal data before determining the appropriate means to reduce them.

Finally, he has to meet specific requirements that apply to its processing and data processed, especially when it comes to sensitive data, when personal data is transferred outside the European Union, etc.

To this end, it is appropriate to adopt a global vision, that goes beyond the framework of the organization's activities and the purposes determined for its processing, and allows to study impacts on individuals concerned by those data.

⁴ Throughout this document the term "privacy" is used as shorthand to refer to "human identity, human rights, privacy, or individual or public liberties".

1. Theory: risk management concepts

Risk management is used in many areas (information security, safety, finance, insurance...). This chapter provides an implementation of this approach in the context of privacy. The methodology presented below is fully compliant with international standards for risk management⁵. It naturally fits into global risk management approaches.

1.1. The notion of privacy risk

In the area of privacy, the only risks to consider are those that processing of personal data pose to privacy. Those **risks** are composed by one feared event (what do we fear?) and all the threats that make it possible (how can this occur?).

Feared events: what has to be avoided

For each processing of personal data, **primary assets** are the following:

- ❑ processes: those of the processing (its features as such, insofar as they deal with personal data) and those required by [Act-I&L] in order to inform the data subjects (Article 32), obtain their consent (if appropriate, Article 7) and allow the exercise of the rights of opposition (Section 38), access (Article 39), correction and deletion (Article 40);
- ❑ personal data: those directly concerned by the processing and those concerned by the processes required by [Act-I&L].



We wish to avoid the following situations⁶:

- ❑ unavailability of legal processes: they do not or no longer exist or work;
- ❑ change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection...);
- ❑ illegitimate access to personal data: they are known by unauthorized persons;
- ❑ unwanted change in personal data: they are altered or changed;
- ❑ disappearance of personal data: they are not or no longer available.

Indeed, occurrence of such events would have **impacts** on the privacy of data subjects, human identity, human rights or civil liberties.



The **feared event** describes the situation and the potential impacts in the considered context.

⁵ Including the international standard [ISO31000].

⁶ Is needed, possible other considerations are:

- "compromise of the processing". Indeed, some processing, such as those involving State security, may need to be kept secret, because knowledge of their existence may cause or aggravate the risk on data subjects;
- "unavailability of the processing" in addition to the "disappearance of personal data". Sometimes it is useful to distinguish the personal data and their processing, which would be indispensable to data subjects, as in the case of certain benefits (health, administrative...);
- "modification of legal process". While this is uncommon and difficult to study, it is possible to appreciate the risks associated with a legal process, for example the one which allow data subjects to exercise their access right, that could change and cause them damage.



Examples of feared events

Data on the habits of employees are illegally collected and used by their superiors to direct research evidence to fire them.

Coordinates are retrieved and used for commercial purposes (spam, targeted advertising...).

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, worsening their condition and even causing disability or death.

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

Threats: what we have to protect from

For a feared event to occur, there must be one or more **risk sources** causing it, accidentally or deliberately. Risk sources may include:

- ❑ persons who belong to the organization: user, computer specialist...
- ❑ persons from outside the organization: recipient, provider, competitor, authorized third party, government organization, human activity surrounding...
- ❑ non-human sources: computer virus, natural disaster, flammable materials, epidemic, rodents...



Risk sources will act, accidentally or deliberately, on the various information system components, on which the primary assets rely. These **supporting assets** may include:

- ❑ hardware: computers, communications relay, USB drives, hard drives...
- ❑ software: operating systems, messaging, databases, business applications...
- ❑ networks: cable, wireless, fiber optic...
- ❑ people: users, administrators, top management...
- ❑ paper media: printing, photocopying...
- ❑ paper transmission channels: mail, workflow...



The action of the risk sources on supporting assets may happen through different **threats**:

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



Examples of threats

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

Level of risks: how to estimate them?

A risk is a scenario that describes how risk sources might exploit supporting assets vulnerabilities leading to cause an incident on primary assets and impacts on privacy.

The **risk level** is estimated in terms of severity and likelihood.

Severity represents the magnitude of a risk. It essentially depends on the level of identification of personal data and the level of consequences of the potential impacts.

Likelihood represents the feasibility of a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing the level of capabilities of the risk sources⁷ to exploit them.

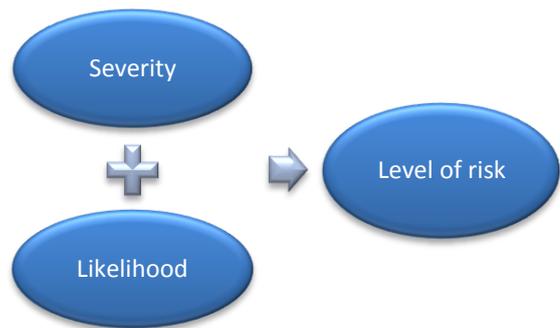


Figure 1 – Determination of the level of each risk

The following figure makes the synthesis of the above-mentioned notions:

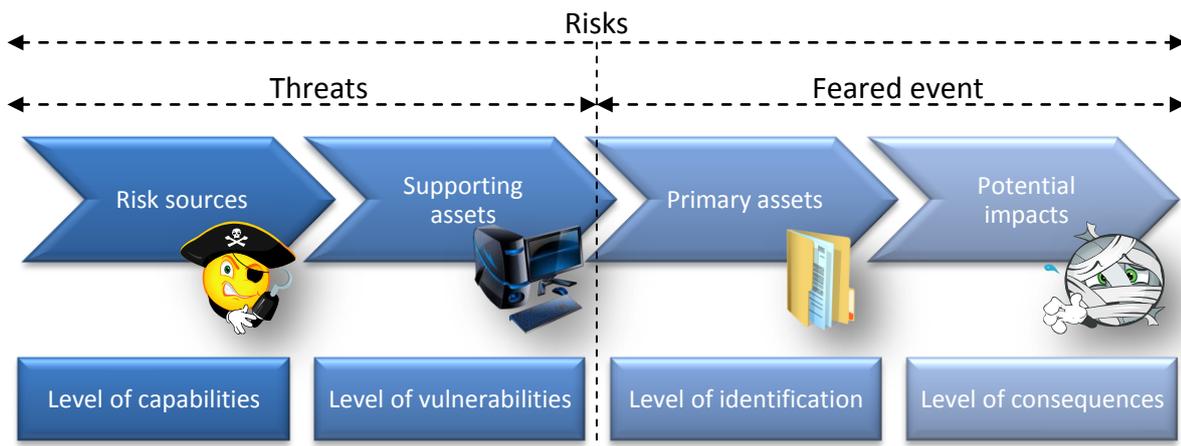


Figure 2 – Risk components

⁷ Capabilities of the risk sources depends on their skills, time available, financial resources, distance to the system, motivation, sense of impunity...

1.2. The privacy risk management approach

The need for managing risks

« The data controller shall 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 »

([\[Act-I&L\]](#) Article 34)

Using a risk management method is the safest way to ensure objectivity and relevance of the choices to make when setting up a processing of personal data.

To assess the risks, feared events have to first be identified and estimated in terms of severity. Then, for those whose severity is high, threats that could lead to the feared events have to be identified and their likelihood estimated. The assessed risks can therefore be treated through proportionate measures. The risks thus assessed can then be treated using commensurate measures.

The approach consists in studying:

1. the context of the processing of personal data,
2. the feared events in this particular context,
3. the possible threats (if needed),
4. the risks involved (if needed),
5. the appropriate measures to treat them.

In addition, this is a continuous improvement process. It therefore requires monitoring changes over time (context, risk, measures...) and updates whenever a significant change occurs.



Figure 3 – The five iterative steps of the approach

Notes

The validation of how risks have been handled as well as the acceptance of residual risk (remaining risks after application of measures), are part of the controller's responsibility. Some risks can neither be neither modified nor retained, especially when sensitive data are processed or when harm that data subjects may suffer is significant. In such cases, it may be necessary to choose to avoid the risks, for example by failing to implement all or part of a processing of personal data.

This approach does not prejudice the conformity assessment that can be made by the CNIL when assessing formalities prior to commencing data processing.

2. Practice: EBIOS in the field of privacy

This chapter describes the approach to be taken in order to analyze the risks posed to privacy by the processing of personal data. It describes how to use the [EBIOS](#)⁸ method in the specific context of data protection.

R

Notes

The approach should be implemented as soon as a new processing operation is designed. Implementing this approach at the outset makes it possible to determine the necessary and sufficient measures and thus to optimize costs. Conversely, implementing it after the creation of the system and the implementation of measures, may call into question choices made. Due to its compatibility with international standards on risk management, this approach can easily be made part of overall risk management.

2.1. Background study: What is the context?

|  | Roles | Stakeholders |
|--|-------------------------------|-------------------------------|
| | Controller ⁹ | Project owner ¹⁰ |
| | Approver ¹¹ | Data controller |
| | Consulted party ¹² | DPO ¹³ and/or CISO |
| | Informed party ¹⁴ | - |

The aim at this stage is to gain a clear view of the scope under consideration by identifying all the useful information for risk management by answering the following questions:

- Which **primary assets need to be protected**?
 - Which processing operation is concerned?
 - What is its purpose (see Articles 6¹⁵ and 9 of [\[Act-I&L\]](#))?
 - Who is it intended for?
 - What business process is executed by this processing operation?
 - Which data subjects are affected by this processing operation¹⁶?
 - How will the legal processes be implemented?

⁸ EBIOS (see acronym on page 28) is the name of the risk management method published by ANSSI (see acronym on page 28). This recognized and proven methodology toolkit is widely used in both the public sector (ministries, organizations under ministerial supervision, communities, etc.) and the private sector (manufacturers, key accounts, consultants, etc.) in France and around the world (Quebec, Belgium, Luxembourg, European Union, NATO, etc.) to manage information system security risks. Its high flexibility and compatibility with international risk management standards allow it to be easily adapted to privacy protection and other needs.

⁹ Person(s) responsible for implementing the action.

¹⁰ May be delegated, represented or contracted out.

¹¹ Legitimate person to approve the action.

¹² Person(s) consulted to obtain useful information for the action.

¹³ Or the person in charge of data protection.

¹⁴ Person(s) informed about the action's results.

¹⁵ The reader is reminded that personal data are collected for specified, explicit and legitimate purposes.

¹⁶ Employees, users, members, customers (current or potential), visitors, patients, students/pupils, etc.

- What kinds of personal data will undergo processing?
- What kinds of personal data will be used by the legal processes?

R

Note

The inventory of personal data must serve as an opportunity to verify whether each item of data is absolutely necessary for the processing operation and whether appropriate storage periods have been set¹⁷.

- What **supporting assets**¹⁸ are used for the primary assets?
 - Which kinds of hardware (computers, routers, electronic media, etc.)?
 - Which kinds of software (operating systems, messaging systems, databases, business applications, etc.)?
 - What are the kinds of computer communications networks (cables, Wi-Fi, fiber optics, etc.)?
 - Who are the individuals involved?
 - Which kinds of supporting paper assets (printouts, photocopies, etc.)?
 - Which paper transmission channels (mail, workflow, etc.)?
- What are the main benefits offered by processing to data subjects or society as a whole?
- What are the main guidelines (regulatory, sectoral, etc.) to be followed?
- What are the relevant sources of risk that might affect¹⁹ the specific context of the processing operation under consideration?
 - Which internal individuals are to be considered (users, administrators, developers, policymakers, etc.)?
 - Which external individuals are to be considered (customers, recipients, providers, competitors, activists, curious persons, malicious individuals, government organizations, surrounding human activity, etc.)?
 - Which non-human sources are to be considered (damaging event, malicious software from an unknown source, natural phenomenon, natural or health disasters, etc.)?

¹⁷ A period "not exceeding the period needed in order to achieve the purposes for which such data are collected and processed" (Article 6 of [\[Act-I&L\]](#)), in the absence of another legal obligation imposing a longer retention period.

¹⁸ Security solutions (products, procedures, measures, etc.) are not supporting assets. They are risk-treatment measures that are determined at the end of the study (encryption, making backups, keeping a log of actions, using a firewall, setting up a virtual private network, informing parties involved, etc.).

¹⁹ These sources may be accidental (blunder, thoughtlessness, poor understanding of commitment, lack of motivation in one's relationship with the organization, etc.) or deliberate (game, ego, revenge, profit motive, etc.).

2.2. Feared events study: What does one fear happening?

|  | Roles | Stakeholders |
|---|-----------------|-----------------|
| | Controller | Project owner |
| | Approver | Data controller |
| | Consulted party | DPO and/or CISO |
| | Informed party | - |

The aim of this step is to obtain a detailed and prioritized list of all feared events that may affect the processing operation under consideration. An example is provided in the table on page 14.

Clarifying feared events requires identifying their **potential impacts**. In other words, what consequences could each feared event have on the identity and privacy of data subjects and human rights or civil liberties if:

- The legal processes were unavailable?
- The processing operation was modified?
- An unauthorized person accessed personal data?
- Personal data were modified?
- Personal data disappeared?

These feared events are ranked by determining their severity based on the level of identification of personal data and the prejudicial effect of these potential impacts.

First of all, the level of **identification** of all personal data (identified beforehand) must be assessed. In other words, how easy is it to identify data subjects²⁰ ?

1. **Negligible**: Identifying an individual using their personal data appears to be virtually impossible (e.g. searching throughout the French population using only an individual's first name).
2. **Limited**: Identifying an individual using their personal data appears to be difficult but is possible in certain cases (e.g. searching throughout the French population using an individual's full name).
3. **Significant**: Identifying an individual using their personal data appears to be relatively easy (e.g. searching throughout the French population using an individual's full name and date of birth).
4. **Maximum**: Identifying an individual using their personal data appears to be extremely easy (e.g. searching throughout the French population using an individual's full name, date of birth and mailing address).

²⁰ "In order to determine whether an individual is identifiable, all means that would allow the said individual to be identified and which are available to or accessible by the data controller or any other person must be taken into consideration" (Article 2 of [\[Act-I&L\]](#)). This includes information that is public, held or obtained otherwise, including over the Internet.

The value of the level that best matches the personal data identified is then selected. Any existing or planned measures that make personal data less easily identifiable should be **listed** as justification as shown in the table on page 14.

Next, the **prejudicial effect** of each feared event should be estimated. In other words, how much damage²¹ would be caused by all the potential impacts?

1. **Negligible**: Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2. **Limited**: Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3. **Significant**: Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).
4. **Maximum**: Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

The value of the level that best matches the potential impacts identified is then selected. Any existing or planned measures that make these potential impacts less harmful should be **listed** as justification as shown in the table on page 14.

Finally, the **severity** is determined by adding the respective personal data level of identification and prejudicial effects of potential impacts values obtained and locating the sum in the table below:

| Level of identification + prejudicial effects | Corresponding severity |
|---|------------------------|
| < 5 | 1. Negligible |
| = 5 | 2. Limited |
| = 6 | 3. Significant |
| > 6 | 4. Maximum |

Table 1 – Determining the severity of each feared event

Option: The severity level thus obtained may be raised or lowered by including additional factors. For example, a large number of data subjects (which can open the door to a massive damaging event) may raise the level of severity by one. A large number of interconnections (especially with foreign sites) or recipients (which facilitates the correlation between originally separated personal data) might also be considered as an aggravating factor. Conversely, a very small number of data subjects or very few or no interconnections or recipients might lower the severity level by one.

²¹Damage to data subjects may be:

- physical (loss of amenity, disfigurement, or economic loss related to physical integrity),
- material (loss incurred or lost revenue with respect to an individual's assets),
- moral (physical or emotional suffering, disfigurement or loss of amenity, etc.).



Tool

The result of this step can be summarized in a table such as the one below:

| Feared events | Level of identification of personal data ²² | Most serious potential impacts | Prejudicial effects of potential impacts | Existing or planned measures | Maximum severity |
|---|--|--|--|---------------------------------------|------------------|
| 1. Unavailability of legal processes | 4. Maximum | <ul style="list-style-type: none"> ✓ Uncontrolled circulation of personal data ✓ Inability to exercise one's rights ✓ Blocking from purchasing procedures | 2. Limited | No planned severity-reduction measure | 3. Significant |
| 2. Change in processing | 4. Maximum | <ul style="list-style-type: none"> ✓ Unsolicited messages/mail from advertisers | 1. Negligible | No planned severity-reduction measure | 2. Limited |
| 3. Illegitimate access to personal data | 4. Maximum | <ul style="list-style-type: none"> ✓ Account theft ✓ Use for commercial purposes | 3. Significant | All data are required | 4. Maximum |
| 4. Unwanted change of personal data | 4. Maximum | <ul style="list-style-type: none"> ✓ Unfulfilled orders | 1. Negligible | Daily backups and retrieval | 2. Limited |
| 5. Disappearance of personal data | 4. Maximum | <ul style="list-style-type: none"> ✓ Must re-register ✓ Loss of benefits | 1. Negligible | Daily backups and retrieval | 2. Limited |

Table 2 – Feared events study

²² In this example, the main types of personal data are customers' marital status, address and bank details as well as products purchased by them and their login ID.

2.3. Threats study: How can it happen? (if needed)

This step may be skipped if the severity level is negligible (1) or limited (2).

|  | Roles | Stakeholders |
|---|-----------------|--------------------------------|
| | Controller | Prime contractor ²³ |
| | Approver | Data controller |
| | Consulted party | DPO and/or CISO |
| | Informed party | - |

The aim of this step is to obtain a detailed, prioritized list of all threats²⁴ that may allow feared events to occur. It is possible to leave out threats relating to feared events of negligible (1) or limited (2) severity. An example is provided in the table on page 17.

Since a threat is a possible action by risk sources on supporting assets, the supporting assets should be identified and estimated for each threat.

First, the **vulnerabilities of the supporting assets** are estimated for each threat. In other words, to what degree can the properties of supporting assets be exploited in order to carry out a threat?

1. **Negligible:** Carrying out a threat by exploiting the properties of supporting assets does not appear possible (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
2. **Limited:** Carrying out a threat by exploiting the properties of supporting assets appears to be difficult (e.g. theft of paper documents stored in a room protected by a badge reader).
3. **Significant:** Carrying out a threat by exploiting the properties of supporting assets appears to be possible (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at reception).
4. **Maximum:** Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy (e.g. theft of paper documents stored in a lobby).

The value of the level that best matches the supporting asset vulnerabilities identified is then selected.

Any existing or planned measures that reduce the vulnerabilities of supporting assets should be **listed** as justification as shown in the table on page 17.

²³ May also be delegated, represented or contracted out.

²⁴ A list of 45 generic threats is provided in the Appendix. Taken from the [EBIOS](#) knowledge bases, these threats are designed to be exhaustive, independent and applied to the specific aspects of privacy protection.

Next, the **capabilities of risk sources** to exploit vulnerabilities (skills, available time, financial resources, proximity to system, motivation, feeling of impunity, etc.) are estimated for each threat.

1. **Negligible**: Risk sources do not appear to have any special capabilities to carry out a threat (e.g. software function creep by an individual acting without malicious intent and who has limited access privileges).
2. **Limited**: The capabilities of risks sources to carry out a threat are limited (e.g.: software function creep by a malicious individual with limited access privileges).
3. **Significant**: The capabilities of risk sources to carry out a threat are real and significant (e.g. software function creep by an individual acting without malicious intent and who has unlimited administration privileges).
4. **Maximum**: The capabilities of risk sources to carry out a threat are definite and unlimited (e.g. software function creep by a malicious individual with unlimited administration privileges).

The value of the level that best matches the risk sources identified is then selected.

Any existing or planned measures that reduce the capabilities of risk sources should be **listed** as justification as shown in the table on page 17.

Finally, the **likelihood** of the threats is determined by adding the values obtained for the vulnerabilities of the supports and the capabilities of the risk sources and locating the sum in the table below:

| Supporting asset vulnerabilities + risk source capabilities | Corresponding likelihood |
|---|--------------------------|
| < 5 | 1. Negligible |
| = 5 | 2. Limited |
| = 6 | 3. Significant |
| > 6 | 4. Maximum |

Table 3 – Determining the likelihood of each threat

Option: The likelihood thus obtained may be raised or lowered by including additional factors. For example, access to the Internet, exchanges of data with foreign sites, interconnections with other systems and a high degree of system heterogeneity or variability may raise the likelihood by one level. Conversely, a homogeneous, stable system that has no interconnections and is closed off from the Internet may lower the likelihood by one level.



Tool

The result of this step can be added to the feared events table from the previous step:

| Feared events | Most likely threats | Supporting asset vulnerabilities | Risk source capabilities | Existing or planned measures | Maximum likelihood ²⁵ |
|---|---|----------------------------------|--------------------------|--|----------------------------------|
| 1. Unavailability of legal processes | <ul style="list-style-type: none"> ✓ <i>Hardware damage (e.g.: server destruction)</i> ✓ <i>Abnormal use of software (e.g. while handling files)</i> ✓ <i>Departure of an individual (e.g. resignation of the individual who knows the procedures)</i> ✓ <i>Disappearance of paper transmission channels (e.g. change in procedure)</i> | 4. Maximum | 3. Significant | No planned likelihood-reduction measures | 4. Maximum |
| 2. Change in processing | N/A | N/A | N/A | N/A | N/A |
| 3. Illegitimate access to personal data | <ul style="list-style-type: none"> ✓ <i>Hardware theft (e.g. theft of a laptop while on a train)</i> ✓ <i>Software function creep (e.g. for personal use)</i> ✓ <i>Software alteration (e.g.: spreading of viruses)</i> | 3. Significant | 3. Significant | No planned likelihood-reduction measures | 3. Significant |
| 4. Unwanted change of personal data | N/A | N/A | N/A | N/A | N/A |
| 5. Disappearance of personal data | N/A | N/A | N/A | N/A | N/A |

Table 4 – Threats study

²⁵ The likelihood is theoretically determined for each threat; only the highest value is kept.

2.4. Risk study: What is the risk level? (if needed)

This step may be skipped if the severity level is negligible (1) or limited (2).

|  | Roles | Stakeholders |
|---|-----------------|------------------|
| | Controller | Project owner |
| | Approver | Data controller |
| | Consulted party | DPO and/or CISO |
| | Informed party | Prime contractor |

The aim of this step is to obtain a risk map in order to determine the order in which they should be treated.

Since a risk consists of a feared event and all the threats that may allow it to occur:

- its **severity** equals that of the feared event,
- its **likelihood** equals the highest likelihood value of the threats associated with the feared event.

The risks can then be **mapped**:

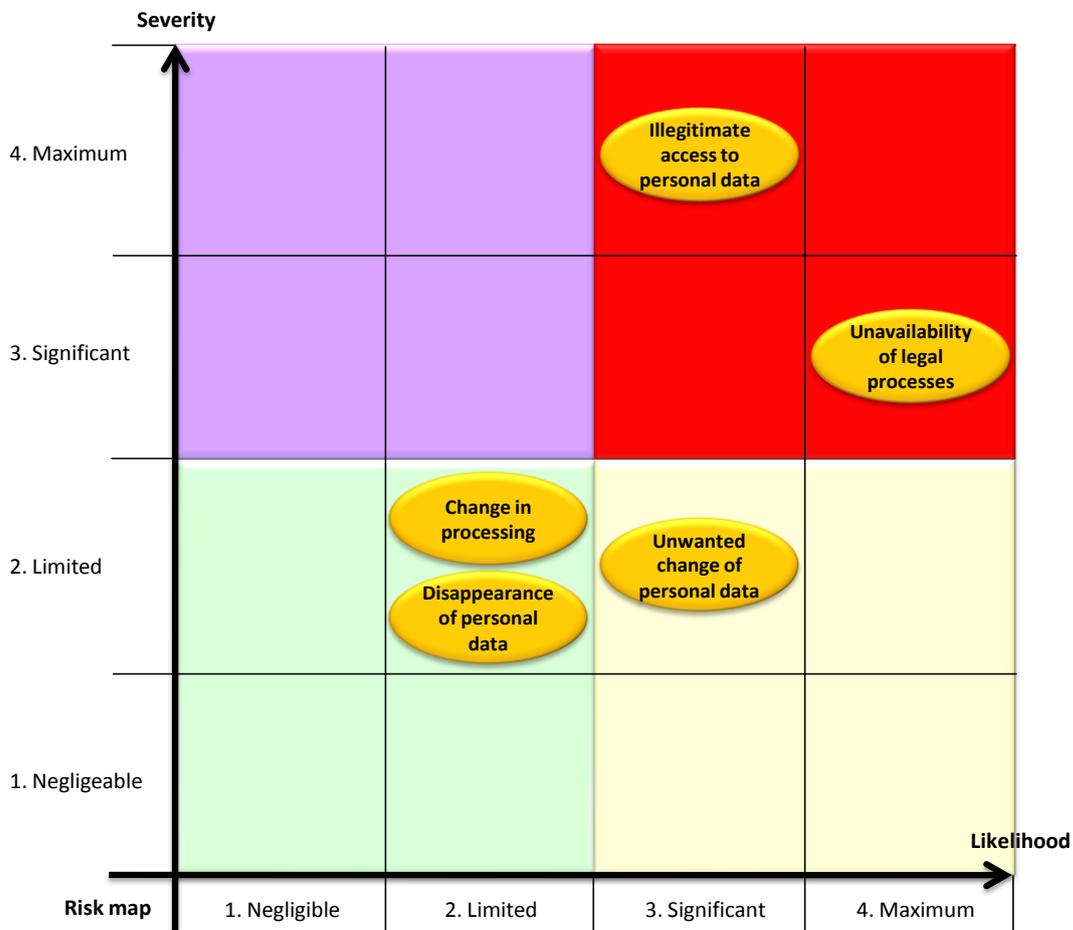


Figure 4 – Risk map

Option: **Objectives** may be set based on where risks are located on the map (in order of priority):

1. **Risks with a high severity and likelihood²⁶** absolutely must be avoided or reduced by implementing security measures that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that these risks are treated by independent measures 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 likelihood²⁷** must be avoided or reduced by implementing security measures that reduce either their severity or their likelihood. Emphasis must be placed on preventive measures.
3. **Risks with a low severity but a high likelihood** must be reduced by implementing security measures that reduce their likelihood. Emphasis must be placed on recovery measures.
4. **Risks with a low severity and likelihood** may be taken, especially since the treatment of other risks should also lead to their treatment.

²⁶ Levels 3 (Significant) and 4 (Maximum).

²⁷ Levels 1 (Negligible) and 2 (Limited).

2.5. Measures study: What can be done to treat risks?

|  | Roles | Stakeholders |
|---|-----------------|---|
| | Controller | Prime contractor or Project owner |
| | Approver | Data controller or CNIL ²⁸ |
| | Consulted party | DPO and/or CISO |
| | Informed party | Project owner or Prime contractor, CNIL |

The aim of this step is to build a protection system that (i) allows risks to be treated in a commensurate manner, that (ii) complies with [\[Act-I&L\]](#) and (iii) is consistent with the data controller's requirements (legal, financial, technical, etc.).

First of all, risk-treatment **measures must be determined**. This is done by linking existing or planned measures (identified earlier in the study or the applicable guidelines) to the risk(s) they help to treat. Subsequent measures are added until the risk level is finally considered acceptable.



Tools

These additional measures may be created from scratch or taken from good practices issued by recognized institutions or international standards. Generally, they must be adapted to the specific context of each processing operation under consideration.

This consists in determining additional measures that will cover:

1. The primary assets: measures designed to prevent security breaches, to detect such breaches or to restore security (informing data subjects, keeping personal data to a minimum, anonymization of personal data, etc.).
2. Then, if the above is insufficient, the potential impacts: measures designed to prevent the consequences of risks from occurring, to identify and limit their effects or to curb them (making of backups, integrity checks, management of personal data breaches, etc.).
3. Then, if the above is insufficient, the risk sources: measures designed to prevent risk sources from acting or making a risk real, to identify and limit their impact or to cause them to backfire (physical and logical access control, activity tracking, management of third parties, protection against malicious codes, etc.);
4. Finally, if the above is insufficient, the supporting assets: measures designed to prevent the exploitation of vulnerabilities, to detect and limit threats that do occur or to restore the normal operating condition (reducing the vulnerabilities of software, hardware, individuals, paper documents, etc.).

Option: It is worth supplementing the system with cross-organizational measures (organization, policy, monitoring, etc.) in order to improve the maturity of personal data protection.

²⁸ In accordance with the legal requirements on prior notification.

Moreover, in order to check the reliability of these measures, it may be worthwhile determining the actions taken in case these measures are ineffective (if they no longer work).



Notes

The higher the capabilities of the risk sources, the more robust measures must be in order to withstand them.

Moreover, any incidents that may have already occurred (especially personal data breaches) as well as any difficulties in implementing certain measures, may be used to improve the security system.

Measures specified must be formally set out, implemented, regularly audited and continually improved.

Next, the severity and likelihood of the **residual risks** (i.e. risks that remain after the selected measures are implemented) should be re-estimated by factoring in these additional measures. They can then be repositioned on the map:

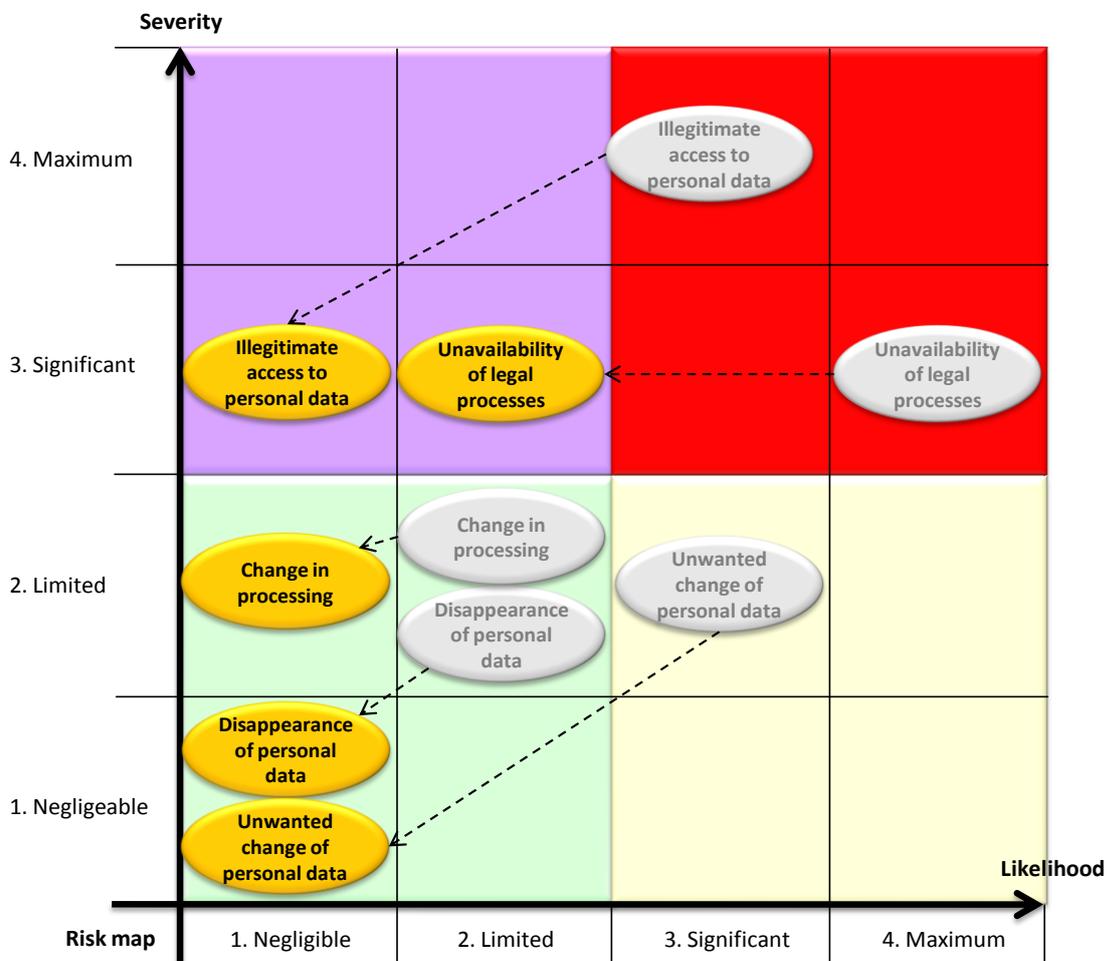


Figure 5 – Residual risk map

Finally, explanations **about why residual risks may be accepted** should be given. These explanations may be based on the new severity and likelihood levels and on the benefits offered by the processing operation identified previously (risk-benefit analysis) by applying the following rules:

1. **Risks with a high severity and likelihood²⁹** must not be taken.
2. **Risks with a high severity but a low likelihood³⁰** may be taken only if it is demonstrated that their severity cannot be reduced and if their likelihood is negligible.
3. **Risks with a low severity but a high likelihood** may be taken only if it is demonstrated that their severity cannot be reduced and if their likelihood is negligible.
4. **Risks with a low severity and likelihood** may be taken.

It may be acceptable to depart from these rules, but only if it is demonstrated that the benefits of processing greatly outweigh the risks.

R

Note

Serious risks may thus be taken if their likelihood is sufficiently low. Certain risks may also be taken if processing makes it possible to save human lives.

²⁹ Levels 3 (Significant) and 4 (Maximum).

³⁰ Levels 1 (Negligible) and 2 (Limited).



Tool

The result of this step, which consists in presenting the measures selected to treat each risk and in re-estimating the severity and likelihood of each risk, may be summarized in a table such as the one below³¹:

| Selected risk-treatment measures ³² | Risks | | | | |
|--|-------------------------|--------------------------------------|---|-------------------------------------|-----------------------------------|
| | 1. Change in processing | 2. Unavailability of legal processes | 3. Illegitimate access to personal data | 4. Unwanted change of personal data | 5. Disappearance of personal data |
| 1. Keep personal data to a minimum | X | | X | X | X |
| 2. Inform data subjects | | X | | | |
| 3. Back up personal data | X | X | | X | X |
| ... | ... | ... | ... | ... | ... |
| Residual severity | 2. Limited | 3. Significant | 3. Significant | 1. Negligible | 1. Negligible |
| Residual likelihood | 1. Negligible | 2. Limited | 1. Negligible | 1. Negligible | 1. Negligible |

Table 5 – Selected risk-treatment measures

The descriptions of the measures may be presented in the following way:

Description of the selected risk-treatment measures

1. Keep personal data to a minimum

Personal data required for processing are identified. It is demonstrated that each item of data is essential.

2. Inform data subjects

Internet users are informed, via the website's order form and in the same font as the rest of the page, of the data controller's identity; the purpose of the processing; whether the information collected is required or optional; the consequences of failing to provide information; the recipients of this information; their rights and the person whom they should contact in order to enforce them; and the planned forms of transmission of this information.

3. Back up personal data

Data on the server are backed up incrementally every day and completely each week. The supporting storage assets are encrypted and stored in a fireproof cabinet. A backup recovery test is performed once a year.

[...]

³¹ The measures should be identified (one per row) and the risk(s) they treat should be indicated (one per column).

³² The measures listed correspond to good practices.

Appendices

Generic threats

Threats that may jeopardize confidentiality

The following table presents the generic threats that can lead to:

- ❑ Illegitimate access to personal data,
- ❑ Compromise of processing (if this feared event is considered).

| Generic threats | Examples of threats | Examples of supporting asset vulnerabilities |
|---|---|--|
| C01. Abnormal use of hardware | 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, etc. | Usable for purposes other than the intended purpose, etc. |
| C02. Hardware espionage | Watching a person's screen without them knowing while on the train; taking a photo of a screen; geolocation of hardware; remote detection of electromagnetic signals, etc. | Allows interpretable data to be observed; generates compromising emanations, etc. |
| C03. Hardware alteration | Tracking by a hardware-based keylogger; removal of hardware components; connection of devices (such as USB flash drives) to launch an OS or retrieve data, etc. | Allows components (boards, expansion cards, etc.) to be added, removed or substituted via connectors (ports, slots, etc.); allows components to be disabled (USB port, etc.) |
| C04. Hardware loss | Theft of a laptop from a hotel room; theft of a professional cellphone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc. | Small, appealing targets (market value), etc. |
| C05. Software function creep | Content scanning; illegitimate cross-referencing of data; raising of privileges, wiping of usage tracks; sending of <i>spam</i> via an e-mail program; misuse of network functions, etc. | Makes data accessible for viewing or manipulation (deletion, modification, movement, etc.); may be used for other than normal purposes; allows the use of advanced functionalities, etc. |
| C06. Software analysis | 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, etc. | Possibility of observing the functioning of software; access to and reading of source codes, etc. |
| C07. Software alteration | Tracking by a software-based key logger; infection by malicious code; installation of a remote administration tool; substitution of components, etc. | Editable (improvable, configurable, etc.); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources, etc.); does not function properly or as expected, etc. |
| C08. Eavesdropping of computer channels | Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc. | Permeable (generation of compromising emanations); allows interpretable data to be observed, etc. |
| C09. Remote espionage of individuals | Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings, etc. | People who cannot keep things to themselves, are predictable (with routine lives that make repeated espionage easy), etc. |
| C10. Manipulation of individuals | Influence (phishing, social engineering, bribery, etc.), pressure (blackmail, psychological harassment, etc.), etc. | Easily influenced (naive, gullible, obtuse, low self-esteem, little loyalty, etc.), easily manipulated (vulnerable to pressure placed on themselves or their circle of family and friends), etc. |
| C11. Acquisition of individuals | Employee poaching; assignment changes; takeover of all or part of the organization, etc. | Little loyalty to the organization; personal needs that are largely unmet; easy breach of contractual obligations, etc. |
| C12. Viewing of paper documents | Reading, photocopying, photographing, etc. | Allows interpretable data to be seen, etc. |
| C13. Theft of paper documents | Theft of files from offices; theft of mail from mailboxes; retrieval of discarded documents, etc. | Portable, etc. |
| C14. Espionage of paper transmission channels | Reading of signature books in circulation; reproduction of documents in transit, etc. | Observable, etc. |

Table 6 – Threats that may jeopardize confidentiality

Threats that may jeopardize integrity

The following table presents the generic threats that can lead to:

- ❑ Changes in processing,
- ❑ Unwanted changes of personal data,
- ❑ Alterations to legal processes (if this feared event is considered).

| Generic threats | Examples of threats | Examples of supporting asset vulnerabilities |
|---|--|--|
| I01. Hardware alteration | Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of an application, etc. | Allows components (boards, expansion cards, etc.) to be added, removed or substituted via connectors (ports, slots, etc.); allows components to be disabled (USB port, etc.) |
| I02. Abnormal use of software | Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc. | Makes data accessible for viewing or manipulation (deletion, modification, movement, etc.); may be used for other than normal purposes; allows the use of advanced functionalities, etc. |
| I03. Software alteration | Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc. | Editable (improvable, configurable, etc.); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources, etc.); does not function properly or as expected, etc. |
| I04. Man-in-the-middle attack via computer channels | <i>Man-in-the-middle attack</i> to modify or add data to network traffic; replay attack (resending of intercepted data), etc. | Allows traffic to be altered (interception then resending of data, either unaltered or altered, etc.); sole means of traffic transmission; allows the computer channel-sharing rules to be changed (transmission protocol authorizing the addition of nodes, etc.), etc. |
| I05. Work overload | High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc. | Insufficient resources for assigned tasks; capacities not suited to working conditions; insufficient skills for carrying out duties Inability to adapt to change, etc. |
| I06. Manipulation of individuals | Influence (rumor, disinformation, etc.), etc. | Easily influenced (naive, gullible, obtuse, etc.), etc. |
| I07. Forgery of paper documents | Changes to figures in a file; replacement of an original by a forgery, etc. | Falsifiable (paper documents with editable content, etc.), etc. |
| I08. Manipulation of paper transmission channels | Changes to a memo without the author's knowledge; change from one signature book to another; sending of multiple conflicting documents, etc. | Allows distributed documents to be altered; sole means of distributing paper documents; allows the paper transmission channel to be altered, etc. |

Table 7 – Threats that may jeopardize integrity

Threats that may jeopardize availability

The following table presents the generic threats that can lead to:

- ❑ Unavailability of legal processes,
- ❑ Disappearance of personal data,
- ❑ Unavailability of processing (if this feared event is considered).

| Generic threats | Examples of threats | Examples of supporting asset vulnerabilities |
|--|--|--|
| A01. Hardware function creep | Storage of personal files; personal use, etc. | Usable for purposes other than the intended purpose, etc. |
| A02. Hardware overload | Storage unit full; power outage; processing capacity overload; overheating; excessive temperatures, etc. | 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, etc. |
| A03. Hardware alteration | Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of the system, etc. | Allows components (boards, expansion cards, etc.) to be added, removed or substituted via connectors (ports, slots, etc.); allows components to be disabled (USB port, etc.) |
| A04. Hardware damage | Flooding, fire, vandalism, damage from natural wear and tear, storage device malfunction, etc. | Poor-quality components (fragile, easily flammable, poor aging resistance, etc.); not suited to the conditions of use; erasable (vulnerable to magnetic fields or vibrations, etc.), etc. |
| A05. Hardware loss | Theft of a laptop or cellphone; disposal of a device or hardware, etc. | Portable, appealing targets (market value), etc. |
| A06. Abnormal use of software | Erasure of data; use of counterfeit or copied software; operator errors that delete data, etc. | Makes data accessible for viewing or manipulation (deletion, modification, movement, etc.); may be used for other than normal purposes; allows the use of advanced functionalities, etc. |
| A07. Software overload | Exceeding of database size; injection of data outside the normal range of values, etc. | 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, etc. |
| A08. Software alteration | Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc. | Editable (improvable, configurable, etc.); insufficiently skilled developers or maintainers (incomplete specifications, few internal resources, etc.); does not function properly or as expected, etc. |
| A09. Deletion of all or part of a software program | Erasure of a running executable or source codes; logic bomb, etc. | Possibility of erasing or deleting programs; sole copy; complex in terms of use (not very user-friendly, few explanations, etc.), etc. |
| A10. Loss of software | Non-renewal of the license for software used to access data, etc. | Sole copy (of license agreements or software, developed internally, etc.); appealing (rare, innovative, high commercial value, etc.); transferable (full transfer clause in license, etc.), etc. |
| A11. Computer channel overload | Misuse of bandwidth; unauthorized downloading; loss of Internet connection, etc. | Non-scalable transmission capacities (insufficient bandwidth; limited amount of telephone numbers, etc.), etc. |
| A12. Computer channel damage | Cut wiring, poor Wi-Fi reception, etc. | Alterable (fragile, breakable, poor cable structure, bare cables, disproportionate sheath, etc.), sole, etc. |
| A13. Computer channel disappearance | Theft of copper cables, etc. | Appealing targets (market value of cables, etc.), carryable (lightweight, may be hidden, etc.); inconspicuous (easily forgotten, trivial, do not stand out, etc.), etc. |
| A14. Work overload | High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc. | Insufficient resources for assigned tasks; capacities not suited to working conditions; insufficient skills for carrying out duties; inability to adapt to |

| Generic threats | Examples of threats | Examples of supporting asset vulnerabilities |
|---|---|---|
| | | change, etc. |
| D15. Personal injury | Occupational accident; occupational disease; other injury or disease; death; neurological, psychological or psychiatric ailment, etc. | Physical, psychological or mental limits |
| D16. Departure of a person | Reassignment; contract termination or dismissal; takeover of all or part of the organization, etc. | Little loyalty to the organization; personal needs that are largely unmet; easy breach of contractual obligations, etc. |
| A17. Erasure of paper documents | Gradual erasure over time; voluntary erasure of portions of a document, etc. | Editable (paper document with erasable content), etc. |
| A18. Damage to paper documents | Aging of archived documents; burning of files during a fire, etc. | Poor-quality components (fragile, easily flammable, poor aging resistance, etc.); not suited to the conditions of use, etc. |
| D19. Disappearance of paper documents | Theft of documents; loss of files during a move; disposal, etc. | Portable, etc. |
| A20. Overload of paper transmission channels | Mail overload; overburdened validation process, etc. | Existence of quantitative or qualitative limits, etc. |
| A21. Damage to paper transmission channel | End of workflow following a reorganization; mail delivery halted by a strike, etc. | Unstable, sole, etc. |
| A22. Alteration of paper transmission channels | Change in how mail is shipped Reorganization of paper transmission channels; change in working language, etc. | Editable (replaceable, etc.), etc. |
| A23. Disappearance of paper transmission channels | Elimination of a process following a reorganization; loss of a document delivery company, etc. | Unrecognized need, etc. |

Table 8 – Threats that may jeopardize availability

Acronyms

| | |
|--------------|---|
| ANSSI | <i>Agence Nationale de la Sécurité des Systèmes d'Information</i> (the French Network and Information Security Agency) |
| CNIL | <i>Commission Nationale de l'Informatique et des Libertés</i> (the French Data Protection Authority). |
| EBIOS | <i>Expression des Besoins et Identification des Objectifs de Sécurité</i> – Expression of needs and identification of security objectives |
| CISO | Chief Information Security Officer |
| IS | Information Security |

Definitions

Controller *The following terms and definitions are considered as equal for the purpose of this document:*

'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law. [\[Directive-1995-46\]](#)

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. [\[Act-I&L\]](#)

'PII controller': privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes. [ISO29100]

Data subject *The following terms and definitions are considered as equal for the purpose of this document:*

An identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [\[Directive-1995-46\]](#)

The 'data subject' of a processing of personal data means an individual

to whom the data covered by the processing relate. [\[Act-I&L\]](#)

'PII principal': natural person to whom the personally identifiable information (PII) relates. [ISO29100]

Feared event Incident that affects availability, integrity or confidentiality of the primary assets.

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

Measure Action to be taken to treat risks. It may be to avoid, modify/reduce, share/transfer or retain them.

Personal data *The following terms and definitions are considered as equal for the purpose of this document:*

'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [\[Directive-1995-46\]](#)

'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 him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration. [\[Act-I&L\]](#)

'Personally identifiable information (PII)': any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal. [ISO29100]

Personal data breach A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community. [\[Directive-2009-136\]](#)

Primary asset Process (those of the processing of personal data and those required by [\[Act-I&L\]](#)) or data (processed or used by legal process) whose availability, integrity or confidentiality has to be protected.

Processing of personal data *The following terms and definitions are considered as equal for the purpose of this document:*

'Processing of personal data' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. [[Directive-1995-46](#)]

'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 otherwise making available, alignment or combination, blocking, deletion or destruction. [[Act-I&L](#)]

'Processing of PII': operation or set of operations performed upon personally identifiable information (PII). [ISO29100]

| | |
|-------------------------|---|
| Risk | Scenario describing a feared event and all threats that make it possible. It is estimated in terms of severity and likelihood. |
| 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 measures), accepting residual risks, communicating (stakeholder consultation, results presentation...), and monitoring changes over time (context, risk, measures...). |
| Risk source | Person or non-human source that can cause a risk, accidentally or deliberately. |
| Severity | Estimation of the magnitude of potential impacts on the data subjects' privacy. It essentially depends on the level of identification of the personal data and prejudicial effect of the potential impacts. |
| Supporting asset | Asset on which some primary assets rely. It can be hardware, software, networks, people, paper or paper transmission channels. |
| Threat | Typical action used by risk sources that may cause a feared event. |
| Vulnerability | Characteristic of a supporting asset, that can be used by risk sources and allowing threats to occur. |

References

- [\[Directive-1995-46\]](#) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- [\[Directive-2002-58\]](#) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)³³.
- [\[Directive-2009-136\]](#) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
- [\[Act-I&L\]](#) Act n°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties³⁴.
- [\[ISO29100\]](#) ISO/IEC 29100:2012, Information technology — Security techniques — Privacy framework, ISO.
- [\[ISO31000\]](#) ISO 31000:2009 – Principles and Guidelines on Implementation, ISO.
- [\[EBIOS\]](#) *Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS* – Expression of needs and identification of security objectives, risk management methodology, 25 January 2010, ANSSI.
- [\[CNIL-SecPersonalData\]](#) Guide « *Security of Personal Data* », edition 2010, CNIL.

³³ Amended by [\[Directive-2009-136\]](#).

³⁴ Amended by the following laws:

- Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data;
- Act of 13 May 2009 relative to the simplification and clarification of law and lighter procedures;
- Law no.2009-526 dated 13/05/2009;
- Organic Law no.2010-704 dated 28/06/2010;
- Law no.2011-334 dated 29 March 2011 relative to the Défenseur des droits;
- Ordinance no.2011-1012 dated 24/08/2011.

Amended by French Act No. 2004-801 of August 6, 2004, on the protection of individuals with 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.