

# Privacy Impact Assessment (PIA)

## METHODOLOGY



## Contents

---

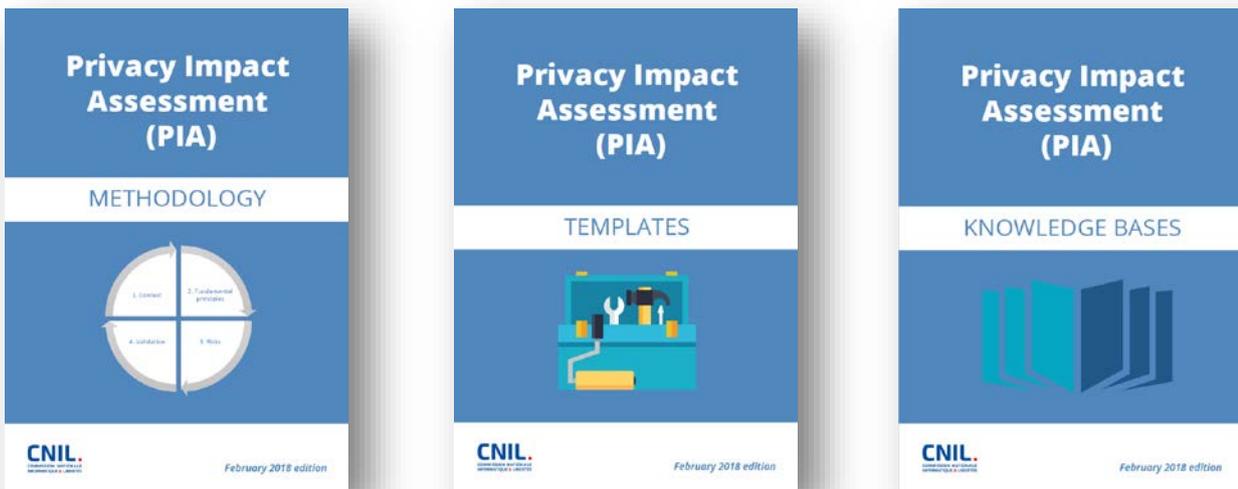
<b>Foreword</b> .....	<b>1</b>
<b>Introduction</b> .....	<b>2</b>
<b>How is a PIA carried out?</b> .....	<b>3</b>
<b>1 Study of the context</b> .....	<b>4</b>
1.1 Overview .....	4
1.2 Data, processes and supporting assets .....	4
<b>2 Study of the fundamental principles</b> .....	<b>5</b>
2.1 Assessment of the controls guaranteeing the proportionality and necessity of the processing 5	5
2.2 Assessment of controls protecting data subjects' rights .....	5
<b>3 Study of the risks related to the security of data</b> .....	<b>6</b>
What is a privacy risk? .....	6
3.1 Assessment of existing or planned controls .....	7
3.2 Risk assessment: potential privacy breaches .....	7
<b>4 Validation of the PIA</b> .....	<b>8</b>
4.1 Preparation of the material required for validation .....	8
4.2 Formal validation .....	8
<b>Appendices</b> .....	<b>9</b>
Definitions .....	9
Bibliography .....	10
Cover of the criteria of the [WP29-Guidelines] .....	11

## Foreword

The methodology of the French Data Protection Authority (CNIL) comprises three guides: one setting out the approach, a second containing facts that could be used for formalising the analysis and a third providing knowledge bases (a catalogue of controls aimed at complying with the legal requirements and treating the risks, and examples):

These can be downloaded from the CNIL's website:

<https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual>



Writing conventions for all of these documents:

- ❑ the term "**privacy**" is used as shorthand to refer to all fundamental rights and freedoms (particularly those mentioned in the [\[GDPR\]](#), by Articles 7 and 8 of the [\[EU Charter\]](#) and Article 1 of the [\[DP-Act\]](#): "privacy, human identity, human rights and individual or public liberties");
- ❑ the acronym "**PIA** " is used interchangeably to refer to Privacy Impact Assessment and Data Protection Impact Assessment (DPIA);
- ❑ wordings in square brackets ([title]) correspond to references.

## Introduction

---

**This guide explains how to carry out a "data protection impact assessment" (see Art. 35 of the [\[GDPR\]](#)), which is more commonly referred to as a Privacy Impact Assessment (PIA).**

It describes how to use the [\[EBIOS\]](#)<sup>1</sup> method in the specific context of "Personal Data Protection". The approach is in keeping with the criteria of the [\[WP29-Guidelines\]](#) (see the appended cover demonstration) and compatible with the international standards on risk management (such as [\[ISO 31000\]](#)).

This is an iterative methodology, which should guarantee a reasoned, reliable use of personal data during processing.

The methodology does not address the initial conditions which determine whether or not a PIA needs carrying out (see Art. 35.1 of the [\[GDPR\]](#)) or the subsequent conditions which determine whether or not the supervisory authority needs consulting (see Art. 36.1 of the [\[GDPR\]](#)).

Performed in principle by a data controller, the purpose of a PIA is to build and demonstrate the implementation of privacy protection principles so that data subjects retain control over their personal data.

It is intended for data controllers who wish to demonstrate their compliance approach and the controls they have selected (concept of accountability, see Art. 25 of the [\[GDPR\]](#)), as well as for product providers wishing to show that their solutions do not breach privacy thanks to a design that respects privacy (concept of Privacy by Design, see Art. 25 of the [\[GDPR\]](#))<sup>2</sup>. It is useful to all stakeholders involved in creating or improving processing of personal data or products:

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

---

<sup>1</sup> EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité (Expression of Needs and Identification of Security Objectives) – is the name of the risk management methodology published by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI/French National Cybersecurity Agency).

<sup>2</sup> In the rest of the document, the term "processing of personal data" is interchangeable with the term "product".

## How is a PIA carried out?

The compliance approach implemented by carrying out a PIA is based on two pillars:

1. **fundamental rights and principles**<sup>3</sup>, which are “non-negotiable”, established by law and which must be respected, regardless of the nature, severity and likelihood of risks;
2. **management of data subjects’ privacy risks**<sup>4</sup>, which determines the appropriate technical and organisational controls to protect personal data<sup>5</sup>.



Figure 1 – Compliance approach using a PIA

To summarise, to carry out a PIA it is necessary to:

1. define and describe the **context** of the processing of personal data under consideration;
2. analyse the controls guaranteeing compliance with the **fundamental principles**: the proportionality and necessity of processing, and the protection of data subjects’ rights;
3. assess privacy **risks** associated with data security and ensure they are properly treated;
4. formally document the **validation** of the PIA in view of the previous facts to hand or decide to revise the previous steps.

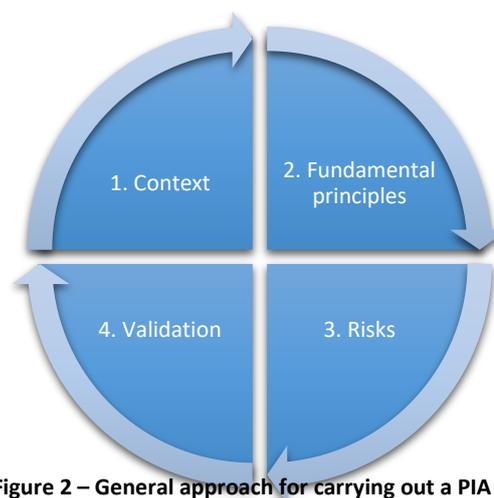


Figure 2 – General approach for carrying out a PIA

**This is a continuous improvement process.**

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

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

<sup>3</sup> Specified, explicit and legitimate purpose; adequate, relevant and non-excessive data; clear and full information for data subjects; limited storage duration; right of access, to object, rectification and erasure, etc.

<sup>4</sup> Related to the security of personal data and having an impact on data subjects’ privacy.

<sup>5</sup> In order to "take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties" (Article 34 of the [IDP-Act](#)).

# 1 Study of the context

 Generally carried out by the project owner<sup>6</sup>, with the help of a person in charge of “Data protection” aspects<sup>7</sup>.

 Aim: gain a clear overview of the personal data processing operations under consideration.

## 1.1 Overview

- Present a brief outline of the **processing** under consideration, its **nature, scope, context, purposes** and **stakes**<sup>8</sup>.
- Identify the **data controller** and any **processors**.
- List the **references applicable** to the processing, which are necessary or must be complied with<sup>9</sup>, not least the approved codes of conduct (see Art. 40 of the [\[GDPR\]](#)) and certifications regarding data protection (see Art. 42 of the [\[GDPR\]](#))<sup>10</sup>.

## 1.2 Data, processes and supporting assets

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

---

<sup>6</sup> In the business sense. This may be delegated, represented or processed by another stakeholder.

<sup>7</sup> Such as the data protection officer for example.

<sup>8</sup> Answer the question "What are the expected benefits (for the organization, for the data subjects, for society in general, etc.)?".

<sup>9</sup> Depending on the case, they will particularly be useful to demonstrate compliance with fundamental principles, justify controls or prove that they correspond to the state of the art.

<sup>10</sup> Other examples: security policy, sector-specific legal standards, etc.

## 2 Study of the fundamental principles



Generally performed by the project owner, then assessed by a person in charge of “Data protection” aspects.



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

### 2.1 Assessment of the controls guaranteeing the proportionality and necessity of the processing

- ❑ Explain and justify the **choices made to comply with the following requirements**:
  1. **purpose(s)**: specified, explicit and legitimate (see Art. 5.1 (b) of the [\[GDPR\]](#));
  2. **basis**: lawfulness of processing, prohibition of misuse (see Art. 6 of the [\[GDPR\]](#))<sup>11</sup>;
  3. **data minimisation**: adequate, relevant and limited (see Art. 5 (c) of the [\[GDPR\]](#))<sup>12</sup>;
  4. **quality of data**: accurate and kept up-to-date (see Art. 5 (d) of the [\[GDPR\]](#));
  5. **storage periods**: limited (see Art. 5 (e) of the [\[GDPR\]](#)).
- ❑ Check that improving the way in which each point is planned, clarified and justified, pursuant to the [\[GDPR\]](#), is either not necessary or not possible.
- ❑ Where applicable, review their description or propose additional controls.

### 2.2 Assessment of controls protecting data subjects' rights

- ❑ Identify or determine, and describe, the **controls** (existing or planned) **selected to comply with the following legal requirements** (it is necessary to explain how it is intended to implement them):
  1. **information** for the data subjects (fair and transparent processing, see Art. 12, 13 and 14 of the [\[GDPR\]](#));
  2. **obtaining consent**, where applicable<sup>13</sup>: express, can be demonstrated and withdrawn (see Art. 7 and 8 of the [\[GDPR\]](#));
  3. exercising the **right of access and right to data portability** (see Art. 15 and 20 of the [\[GDPR\]](#));
  4. exercising the **rights to rectification and erasure** (see Art. 16 and 17 of the [\[GDPR\]](#));
  5. exercising the **right to restriction of processing and right to object** (see Art. 18 and 21 of the [\[GDPR\]](#));
  6. **processors**: identified and governed by a contract (see Art. 28 of the [\[GDPR\]](#));
  7. **transfers**: compliance with the obligations bearing on transfer of data outside the European Union (see Art. 44 to 49 of the [\[GDPR\]](#)).
- ❑ Check that improving each control and its description, pursuant to the [\[GDPR\]](#), is either not necessary or not possible.
- ❑ Where applicable, review their description or propose additional controls.

<sup>11</sup> Also demonstrate that the recipients are legitimate.

<sup>12</sup> Also demonstrate that the recipients genuinely need to access the data.

<sup>13</sup> Justify the cases where consent has not been obtained.

### 3 Study of the risks related to the security of data<sup>14</sup>

#### What is a privacy risk?

A risk is a hypothetical scenario that describes a feared event and all the threats that would allow this to occur. More specifically, it describes:

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

The following diagram summarises all the concepts above:

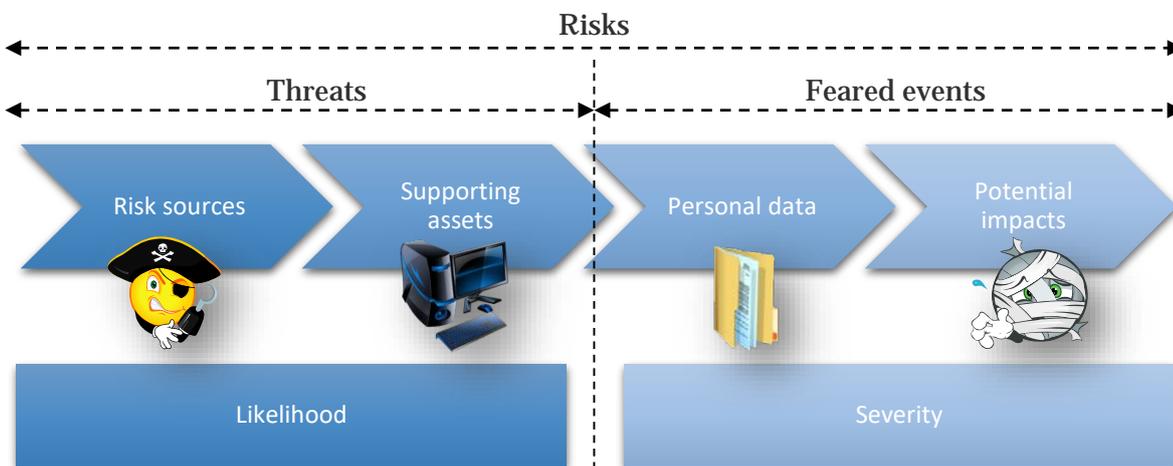


Figure 3 – Risk components

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

- ❑ **severity** represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts<sup>15</sup>;
- ❑ **likelihood** expresses the possibility of a risk occurring. It primarily depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them.

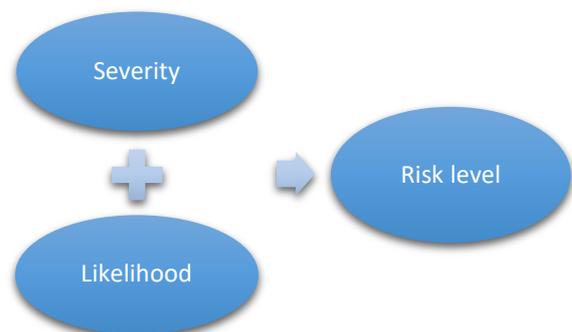


Figure 4 – Factors used to estimate the risks

<sup>14</sup> see Art. 32 of the [\[GDPR\]](#).

<sup>15</sup> In view of the context of the processing of personal data (nature of data, data subjects, purpose of the processing, etc.).

### 3.1 Assessment of existing or planned controls

 Generally performed by the prime contractor<sup>16</sup>, then assessed by a person in charge of “Data security” aspects<sup>17</sup>.

 Objective: gain a good understanding of the controls that contribute to security.

- ❑ Identify or determine the **existing or planned controls** (already undertaken), which can take three different forms:
  1. **controls bearing specifically on the data being processed**: encryption, anonymization, partitioning, access control, traceability, *etc.*;
  2. **general security controls regarding the system in which the processing is carried out**: operating security, backups, hardware security, *etc.*;
  3. **organizational controls (governance)**: policy, project management, personnel management, management of incidents and breaches, relations with third parties, *etc.*
- ❑ Check that improving each control and its description, pursuant to best security practices, is either not necessary or not possible.
- ❑ Where applicable, review their description or propose additional controls.

### 3.2 Risk assessment: potential privacy breaches

 Generally performed by the project owner, then assessed by a person in charge of “Data protection” aspects.

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

- ❑ For each feared event (illegitimate access to personal data<sup>18</sup>, unwanted change of personal data<sup>19</sup>, and disappearance of personal data<sup>20</sup>):
  1. determine the potential **impacts** on the data subjects’ privacy if it occurred<sup>21</sup>;
  2. estimate its **severity**, particularly depending on the prejudicial nature of the potential impacts and, where applicable, controls likely to modify them;
  3. identify the **threats** to personal data supporting assets that could lead to this feared event<sup>22</sup> and the **risk sources** that could cause it;
  4. estimate its **likelihood**, particularly depending on the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them.
- ❑ Determine whether the risks identified in this way<sup>23</sup> can be considered acceptable in view of the existing or planned controls.
- ❑ If not, propose additional controls and re-assess the level of each of the risks in view of the latter, so as to determine the residual risks.

<sup>16</sup> This may be a delegate, representative or processor.

<sup>17</sup> Chief information security officer or other.

<sup>18</sup> They are known to unauthorised persons (breach of personal data confidentiality).

<sup>19</sup> They are altered or changed (breach of personal data integrity)

<sup>20</sup> They are not or no longer available (breach of personal data availability).

<sup>21</sup> Answer the question "What do we fear might happen to data subjects?".

<sup>22</sup> Answer the question "How might this happen?".

<sup>23</sup> A risk is based upon a feared event and all threats that would make it possible.

## 4 Validation of the PIA

 Generally performed by the controller, with the help of a person in charge of "Data Protection" aspects.

 Objective: decide whether or not to accept the PIA in light of the study's findings.

### 4.1 Preparation of the material required for validation

- Consolidate and present the study's findings:
  1. prepare a visual presentation of the **controls selected to ensure compliance with the fundamental principles**, depending on their compliance with the [\[GDPR\]](#) (e.g.: conditional on improvement or considered compliant);
  2. prepare a visual presentation of the **controls selected to contribute to data security**, depending on their compliance with best security practices (e.g.: conditional on improvement or considered compliant);
  3. visually map the **risks** (initial and residual where applicable<sup>24</sup>) depending on their severity and likelihood;
  4. draw up an **action plan** based on the additional controls identified during the previous steps: for each control, determine at least the person responsible for its implementation, its cost (financial or in terms of workload) and estimated timeframe.
- Formally document the consideration of stakeholders:
  1. the **advice of the person in charge of "Data Protection" aspects** (see Art. 35 (2) of the [\[GDPR\]](#));
  2. the **view of data subjects or their representatives** (see Art. 35 (9) of the [\[GDPR\]](#)).

### 4.2 Formal validation

- Decide on whether the selected controls, residual risks and action plan are acceptable, with justifications, in light of the previously identified stakes and views of the stakeholders. In this way, the PIA may be:
  1. validated;
  2. conditional on improvement (explain in what way);
  3. refused (along with the processing under consideration).
- Where necessary, repeat the previous steps so that the PIA can be validated.

<sup>24</sup> Risks that remain after the controls have been implemented.

## Appendices

---

### Definitions

Note: the words in brackets correspond to the shorter terms used in this document.

<b>Control</b>	Action to be taken.  <i>Note: this may be technical or organisational and may entail putting fundamental principles into practice or avoiding, reducing, transferring or assuming all or part of the risks.</i>
<b>Data controller (controller)</b>	The natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. <a href="#">[GDPR]</a>  <i>Note: unless expressly designated by legislative or regulatory provisions relating to this processing. <a href="#">[DP-Act]</a></i>
<b>Data subjects</b>	Persons to whom the data covered by the processing relate. <a href="#">[DP-Act]</a>
<b>Feared event</b>	Potential data breach likely to have impacts on data subjects' privacy.
<b>Likelihood</b>	Estimation of the possibility for a risk to occur.  <i>Note: this primarily depends on the level of exploitable vulnerabilities and the level of capabilities of the risk sources to exploit them.</i>
<b>Personal data (data)</b>	Any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. <a href="#">[GDPR]</a>  <i>Note: In order to determine whether a person is identifiable, all the means that the data controller or any other person can use or may have access to should be taken into consideration. <a href="#">[DP-Act]</a></i>
<b>Personal data processing (processing)</b>	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. <a href="#">[GDPR]</a>
<b>Risk</b>	Scenario describing a feared event and all threats that make it possible.  <i>Note: it is estimated in terms of severity and likelihood.</i>
<b>Risk source</b>	Person or non-human source that can cause a risk.  <i>Note: this source may act accidentally or deliberately.</i>

<b>Severity</b>	Estimation of the magnitude of potential impacts on the data subjects' privacy. <i>Note: this primarily depends on the prejudicial nature of the potential impacts.</i>
<b>Supporting asset</b>	Asset on which personal data rely. <i>Note: this may be hardware, software, networks, people, paper or paper transmission channels.</i>
<b>Threat</b>	Procedure comprising one or more individual actions on data supporting assets. <i>Note: it is used, intentionally or otherwise, by risk sources and may cause a feared event.</i>

## Bibliography

<b>[EU Charter]</b>	Charter of Fundamental Rights of the European Union, 2010/C 83/02.
<b>[GDPR]</b>	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
<b>[DP-Act]</b>	French Data Protection Act no. 78-17 of 6 January 1978, amended <sup>25</sup> .
<b>[WP29-Guidelines]</b>	Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, Article 29 Working Party.
<b>[EBIOS]</b>	Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS/Expression of needs and identification of security objectives, Risk management methodology, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI/French National Cybersecurity Agency).
<b>[ISO 31000]</b>	ISO 31000:2009, Risk management – Principles and guidelines, ISO.

<sup>25</sup> Amended by French Act No. 2004-801 of 6 August 2004 on the protection of individuals in regard to the processing of personal data, and by French Act No. 2009-526 of 12 May 2009 on the simplification and clarification of French law and the facilitation of procedures.

## Cover of the criteria of the [\[WP29-Guidelines\]](#)

Criteria of the <a href="#">[WP29-Guidelines]</a>	Cover	Chapter in this guide
<p>A systematic description of the processing is provided (Article 35(7)(a):</p> <ul style="list-style-type: none"> <li>- nature, scope, context and purposes of the processing are taken into account (recital 90);</li> <li>- personal data, recipients and period for which the personal data will be stored are recorded;</li> <li>- a functional description of the processing operation is provided;</li> <li>- the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;</li> <li>- compliance with approved codes of conduct is taken into account (Article 35(8)).</li> </ul>	☑	1. Study of the context
<p>Necessity and proportionality are assessed (Article 35(7)(b)):</p> <ul style="list-style-type: none"> <li>- controls envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account: <ul style="list-style-type: none"> <li>- controls contributing to the proportionality and the necessity of the processing on the basis of: <ul style="list-style-type: none"> <li>- specified, explicit and legitimate purpose(s) (Article 5(1)(b));</li> <li>- lawfulness of processing (Article 6);</li> <li>- adequate, relevant and limited to what is necessary data (Article 5(1)(c));</li> <li>- limited storage duration (Article 5(1)(e));</li> </ul> </li> </ul> </li> <li>- controls contributing to the rights of the data subjects: <ul style="list-style-type: none"> <li>- information provided to the data subject (Articles 12, 13 and 14);</li> <li>- rights of access and portability (Articles 15 and 20);</li> <li>- rights to rectify and erase (Articles 16 and 17);</li> <li>- rights to object and restriction of processing (Articles 16 and 21);</li> <li>- processors (Article 28);</li> <li>- safeguards surrounding international transfers (Chapter V).</li> </ul> </li> </ul>	☑	2. Study of the fundamental principles
<p>Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):</p> <ul style="list-style-type: none"> <li>- origin, nature, particularity and severity of the risks are assessed (see recital 84) or, more specifically, for each risk (illegitimate access, unwanted change and disappearance of data), from the perspective of the data subjects: <ul style="list-style-type: none"> <li>- risk sources are taken into account (recital 90);</li> <li>- potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, unwanted change and disappearance of data;</li> <li>- threats that could lead to illegitimate access, unwanted change and disappearance of data are identified;</li> <li>- likelihood and severity are estimated (recital 90);</li> </ul> </li> <li>- controls envisaged to address those risks are determined (Article 35(7)(d) and recital 90).</li> </ul>	☑	3. Study of data security risks
<p>Interested parties are involved:</p> <ul style="list-style-type: none"> <li>- the advice of the DPO is sought (Article 35(2));</li> <li>- the views of data subjects or their representatives are sought (Article 35(9)).</li> </ul>	☑	4. Validation of the PIA