apdcat
Autoritat Catalana de Protecció de Dades

Data Protection Impact Assessment

Update: June 2022

Guides Collection. No 4.

Generalitat de Catalunya

Index

1. Introduction

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 and on the free movement of such data, in short, the General Data Protection Regulation (RGPD or Regulation), incorporates a new obligation for controllers: to assess the impact of processing operations that are likely to result in a high risk to the rights and freedoms of natural persons.

The reform of the data protection regulation in Europe proposes a new compliance model geared towards responsible data management. It goes beyond the previous model, which was too formalistic in some respects. The new regulation introduces new requirements for data controllers. Among these, accountability is particularly relevant: being compliant is not enough, you must be able to prove that you are. In this respect, data protection impact assessments (AIPD) are a key tool, as they are useful to demonstrate responsible data processing.

For AIPD results to be objective, repeatable and comparable, they must be based on systematic methods. For this reason, we intends to guide the execution of impact assessments, following the provisions in the RGPD.

The regulation takes a risk-based approach to data protection, which requires to conduct risk analysis and, if risks are too high, a risk reduction. We can classify the risks associated with data processing into two types: the risks inherent to the data processing (as it has been designed) and the risks associated with the security of the data.

When risks inherent to the data processing are too high, we need to modify it to reduce them. For example, to completely avoid the processing of some types of data that are particularly sensitive or to restrict access to such data.

Risks associated with data security are those that result from the loss of confidentiality, integrity, and availability of the data. Standard risk analysis methodologies are complex and small organizations may have difficulties to implement them. In this guide, we propose an alternative methodology, which seeks to simplify the analysis. When the computed risk is too high, we must apply security controls to reduce it.

2. General facts about DPIA

Key points

- A data protection impact assessment (DPIA) is a procedure that aims to identify and control the risks associated with a data processing.
- A DPIA is required when the data processing is likely to result in a high risk for the rights and freedoms of natural persons.

2.1 What is a data protection impact assessment?

A data protection impact assessment (DPIA) is a procedure that seeks to identify and control the risks that processing brings to the rights and freedoms of natural persons. DPIAs are also useful instruments in relation to the principle of accountability.

The Regulation establishes the rights that people have regarding the processing of their data (right to information, etc.). When talking about "risks to the rights and freedoms of natural persons", we do not limit ourselves to the rights recognized by the Regulation, but to any effect that the data processing may have on the fundamental rights and freedoms of natural persons: freedom of expression, freedom of thought, prohibition of discrimination, freedom of conscience, freedom of religion, etc.

When identifying risks, we must consider any impact of the data processing on natural persons (physical, economic, emotional, etc.). Some potential impacts are:

- Impossibility to access services or other opportunities.
- Discrimination.
- Theft of identity and other frauds.
- Economic losses.
- Damage to reputation.
- Physical damage.
- Loss of confidentiality.
- Impossibility to exercise any right.

These impacts can be materialized for two main reasons.

- The data processing as it is designed. For example, data processing may thwart the rights and freedoms of a person because the data being processed is particularly sensitive, the people that have access to them, etc.
- The loss of data security; in particular, the loss of data confidentiality, integrity or availability.

To control the risks inherent in the data processing, the controller must establish the necessary controls to ensure that the processing is done according to the GDPR. In particular, the controller must ensure that the processing it is necessary and proportional, and that the necessary mechanisms for natural persons to exercise their rights are properly established.

To keep the risks related to data security under control, the controller has to conduct a risk analysis and then propose security controls that are appropriate to the evaluated risk.

2.2 When do you have to do a DPIA?

The GDPR requires the data controller to conduct a DPIA when data processing is likely to result in a high risk to the rights and freedoms of natural persons. The GDPR does not describe what is meant by high risk; it only gives a list of three cases in which a DPIA is mandatory[1].

Given the lack of specificity of the GDPR, we will follow the procedure described by the WT29, which gives a list of nine criteria to determine if a processing operation is likely to result in high risk (see below). The greater the number of criteria met by the processing, the more likely is it result in a high risk. As a rule of thumb, the WG29 proposes to carry out a DPIA when the processing meets two or more criteria; although, in some cases, a DPIA may be required even if only one criterion is met.

1. Evaluation or scoring, including profiling and predicting, especially from aspects. concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements. Examples:
   - A bank screens its customers against a credit reference database.
   - A biotechnology company offers genetic tests to assess and predict the disease/health risks.
   - A company builds behavioral or marketing profiles based on the usage or navigation on its website.
2. Automated-decision making with legal or other significant effect.
   For example, when the processing may lead to the exclusion or discrimination of natural persons.
3. Systematic monitoring. Processing used to observe, monitor or control data subjects, including data collected through a systematic monitoring of a publicly accessible area. In systematic monitoring, personal data may be collected without data subjects being aware

[1] RGPD, article 35.3

of the fact, of who is collecting their data and of the intended use of the data. Additionally, in public (or publicly accessible) space(s), it may be impossible for individuals to avoid being subject to such processing.

4. Sensitive data. This includes special categories of data as defined in Article 9:

   - Racial or ethnic origin.
   - Political opinions.
   - Religious or philosophical beliefs.
   - Trade union membership.
   - Genetic data.
   - Biometric data processed for the purpose of uniquely identifying a natural person.
   - Data concerning health.
   - Data concerning a natural person's sex life or sexual orientation.

   This criterion also includes:

   - Personal data relating to criminal convictions or offenses.
   - Data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data.
   - Information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information).

5. Data processed on a large scale.
   The GDPR does not define what constitutes large-scale. The WP29 recommends considering the following factors to determine if the processing is carried out on a large scale:

   - The number of data subjects concerned, either as a specific number or as a proportion of the relevant population.
   - The volume of data and/or the range of different data items being processed.
   - The duration, or permanence, of the data processing activity.
   - The geographical extent of the processing activity.

6. Data sets that have been matched or combined.

7. Data concerning vulnerable data subjects.
   The power imbalance between the data subject and the data controller may thwart the ability of the data subject to exercise his or her rights.

- Employees in the processing done by their employer.
- Children.
- Patients.
- Vulnerable segments of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly.

8. Innovative use or applying new technological or organizational solutions.

9. Processing that prevents data subjects from exercising a right or using a service or a contract.
   For example, a bank that screens its clients against a credit reference database in order to decide whether to offer them a loan.

Comments

- In previous versions of the WP28's guidelines on DPIA, there was an additional criterion: data transfers outside the EU boundaries. This criterion was removed in revision 1.
- According to article 35.4 of the GDPR, data protection authorities must publish a list of processing operations that require a DPIA. The common trend is to adopt closely the recommendations done by the WP28 in their guidelines. This is the case of the Catalan authority (APDCAT) and the Spanish authority (AEPD).

Examples

- A hospital that processes health data of its patients.
  Relevant criteria**:**
  - Sensitive data.
  - Large-scale.
  - Vulnerable people.
- The use of cameras to monitor drivers on highways when an intelligent system to recognize license plate numbers is envisaged.
  Relevant criteria:
  - Systematic monitoring**.**
  - Innovative use of technologies**.**
- A company that systematically monitors the activities of its employees: work station, internet activity, etc**.**

Relevant criteria:
- Systematic monitoring.
- Vulnerable people.

- Elaboration of profiles from public data.
  Relevant criteria:
  - Evaluation or scoring.
  - Large-scale.
  - Matching or combining data sets.

Regardless of the risks associated to a data processing, in the following cases there is no need to conduct a DPIA:

- When the nature, extent, context and purpose of the processing are very similar to another processing for which a DPIA has already been performed.
- When a processing in the public interest or to meet a legal obligation has a legal basis in union law or in the law of the member state, and a data protection impact assessment has already been carried out in the context of the adoption of that legal basis.
- When the processing is included in a list of processing operations (published by the competent authority) that do not require a DPIA. At this time, neither the APDCAT nor the AEPD have published such a list.

Comments

- There is no need to conduct a DPIA if the GDPR does not apply.
- The GDPR applies to the processing of personal data done by a company or organization located in the EU or in a place where the EU law is applicable, or by a company or organization located outside the EU if it processes data of EU residents in relation to the supply of goods or services and to control their behavior.

Processing operations can evolve, and such evolution may alter the risks associated to the processing. Similarly, social evolution may alter the perception that we have of the risks associated to a processing operation. These changes may be reflected in the need to perform a DPIA. For example, changes in the organizational structure of the controller may alter the risks, and a society that becomes aware of discrimination against some group alters the perception of risk. In these cases, we need to re-assess the need to conduct a DPIA.

When failing to conduct a DPIA that is mandatory, the processing operation may suffer from undetected risks. These undetected risks have not been analyzed nor assessed, and, consequently, appropriate measures to mitigate the negative effects over the rights and freedoms of the data subjects could not have been adopted. According to article 83 of the GDPR, the failure to conduct a DPIA when it is necessary is a sanctionable infringement.

2.3 How to conduct a DPIA?

2.3.1 At what moment should a DPIA be conducted?

If a DPIA is needed, it must be conducted as soon as possible. In particular, for new processing operations, it must be done before starting to process the data. This follows the data protection by design and by default approach and allows us to use the DPIA as a tool to help decision-making in the design of the processing operation.

For processing operations already underway, a DPIA should be carried out as soon as a serious risk to the rights and freedoms of persons is detected. It should be noted that the DPIAs are not a one-time task, but rather involve an ongoing re-evaluation process. In particular, it is necessary to re-evaluate the need to make a DPIA when significant changes occur in the processing operation or in its context (organizational or social).

2.3.2 Who should be involve in a DPIA?

The controller is the main actor in a DPIA. Despite that other actors may be involved; the controller remains accountable for the task.

The processor, if any, must support the controller when conducting a DPIA.

When conducting a DPIA, the controller must seek the advice of the data protection officer (DPO). This advice must be documented in the DPIA. In particular, the controller must request the opinion of the DPO in the following topics:

- To determine if a DPIA is required.
- The methodology used to conduct the DPIA.
- To determine if the DPIA should be conducted internally or outsourced.
- Measures that need to be taken to protect the rights and freedoms of people.
- To determine if the DPIA has been carried out correctly and if the conclusions meet the data protection requirements.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing. If seeking such views is deemed inappropriate, it should be documented in the DPIA. For example, because seeking such views has a disproportionate cost, is impossible, or may jeopardize the confidentiality of a business plan.

The opinion of the interested parties can be collected in different ways: surveys, question a representative of the data subjects, etc. In any case, the controller must have a legal basis to process any personal information that is generated when collecting these views.

Apart from the previous actors, it may be necessary to involve several internal or external, such as units or specific areas of the organization, independent experts, security officers, etc.

2.3.3 Wich is the minimum content of a DPIA?

The result of an impact assessment is a report, a set of documentation, that includes the characteristics of the processing operation evaluated and the decisions taken to mitigate its risks, in accordance with a risk identification and assessment. Based on these risks, the necessity and proportionality of the processing are also assessed.

The GDPR establishes the minimum content of DPIAs as follows:

- Description of the processing operations.
- Assessment of the necessity and the proportionality of the processing.
- Evaluation of the risk for the rights and freedoms of data subjects.
- Measures taken to mitigate the identified risks.

2.3.4 Which are the phases of a DPIA?

A DPIA must follow a systematic process. In this guide, we propose a methodology that comprises the following phases:

1. To assess the necessity of conducting a DPIA. Although this assessment should be done prior to starting the DPIA, to leave evidence of the fact that it has been done, we devote the first section of the DPIA to it. This is particularly relevant when the assessment concludes that a DPIA is not required.

2. Systematic description of the processing. The description of the processing and the context in which it takes place is essential to determine the risks involved.

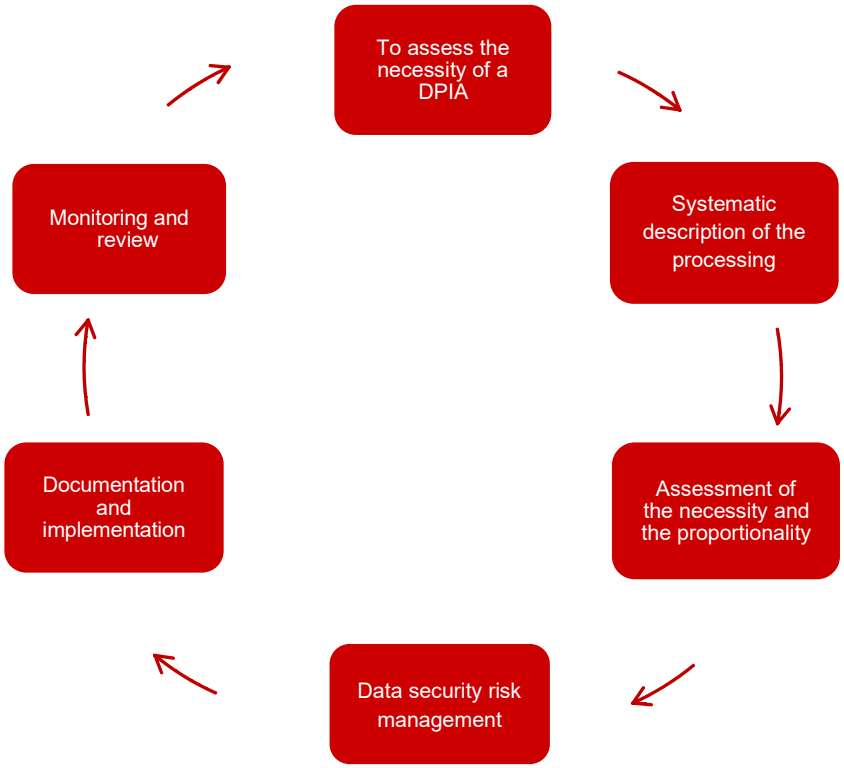
3. Assessment of the necessity and proportionality of the processing. Given a purpose, we need to design the processing operation that is the least intrusive in achieving the

purpose (necessity). The benefit of the processing must be greater than the potential harm (proportionality).

4. Data security risk management. We must evaluate the risk to the rights and freedoms of data subjects related to a violation of data security. The risk results from combining the impact and the likelihood of security violations. The higher the risk, the more exhaustive the security controls must be.

5. Documentation and implementation. The result of a DPIA is a document that describes the tasks performed in the previous points. Once this is documented, we need to take the necessary steps to implement the proposed measures to safeguard the rights and freedoms of data subjects.

6. Monitoring and revision. The DPIA does not end when the documentation and implementation are completed. Ongoing monitoring of the processing operation is needed to detect changes in its risks (either because of modifications introduced in the processing operation or the perception of risk), which may trigger the need to revise the DPIA.



2.4 What to do if the DPIA concludes a high risk?

According to article 36, if the DPIA concludes that the processing operation introduces a high risk for the rights and freedoms of the data subjects, the controller must consult the supervisory authority before starting the processing.

Once the supervisory authority has all the necessary documentation, it must respond in writing within eight weeks. This period may be extended by six weeks, considering the complexity of the intended processing.

In the context of prior consultation, the data protection authority may use any of the powers included in article 58 of the GDPR, both research and corrective measures, such as "to impose a temporary or definitive limitation including a ban on processing".

3. Systematic description of the processing

Key points

- To be able to assess the risks for the rights and freedoms associated with processing, it is essential to have a systematic description of it.
- We propose a list of questions that will help the controller in this description. The aim of these questions is to emphasize relevant aspects about the risks

To accurately determine the risks that affect a processing operation, we need to know in detail the processing operation and its context. We propose a list of questions, as a guide that the controller can use to describe the treatment. These questions aim at highlighting aspects that can be key in determining the risks of the processing[2].

3.1 Which is the processing operation?

The purpose of this question is to delimit the processing operation, at the same time that a first description is made.

[2] Guidelines for SME on the security of personal data processin, ENISA, December 2016

Which processing operations can be evaluated in a DPIA ?

A DPIA can refer to one or multiple processing operations if they are similar in terms of data types, scope, context, purpose, and risks.

A DPIA can also be used to evaluate the impact of an application or processing platform. The controller is not free from conducting a DPIA for processing operations that make use of such an application or platform, but it can be based on the DPIA of the application or platform

Examples

- A hospital manages medical data of the patients: medical history, contact data, etc.
- The human resources system of a company manages personal data of its employees: contact data, bank details, compensation, periods of leave and holidays.

3.2 What is the purpose of the processing?

According to the RGPD, the purpose of a data processing must be explicit, legitimate and determined before collecting the data.

Requiring the controller to specify the purpose of the processing before it starts, helps the data subjects understand how their data will be used. This way, data subjects can make informed decisions regarding the use of their data. In addition, it avoids the use of the collected data for non-compatible purposes.

The purpose limitation principle is closely related to other principles, such as lawfulness, fairness, and transparency. Transparency requires data subjects to be appropriately informed about the use of their data. Lawfulness and fairness cannot be assessed if the purpose is unknown.

Example

- A company processes the data of its clients for accounting purposes.
- The marketing department of a company wants to use the data of its clients for advertising purposes.

Although the previous cases may process the same data, the purpose is very different. The difference in purpose is very relevant; for instance, to determine the legal basis of the processing. In the first case, the controller processes the data to comply with a legal obligation. In the second case, the legal basis is consent.

3.3 Types and characteristics of the processed data

This question is related to the description of the processing operation (done in question 1); however, due to its relevance, we devote this item to specifying the types and characteristics of the data to be treated. Among other things, this information is important when determining the risks associated with the processing operation and when determining the lawfulness of the operation.

We highlight the following characteristics of the data:

3.3.1 Data source

We tell whether the data were obtained directly from the data subject or from a third party and, if so, specify it.

3.3.2 Storage period

Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) subject to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of the data subject.

3.3.3 Special categories of data

By the term "special categories of data", the GDPR refers to data types that, by their very nature, present greater risks for the rights and freedoms of individuals. The GDPR has stricter limits for the processing of these types of data.

Special categories of data include:

- Ethnic or racial origin.
- Political opinions.
- Religious or philosophical convictions.
- Union affiliation.
- Genetic data.
- Biometric data capable of uniquely identifying a person.
- Facts about health.
- Facts about a person's life or sexual orientation.

Although not a special category of data, data related to convictions or criminal offenses is also subject to further processing restrictions.

Similarly, data of vulnerable people (in particular, children) also receive special protection.

3.3.4 Processing of data for a different purpose

To process data for a purpose other than the one that motivated the collection, we must make sure that the purpose is compatible or that there are other circumstances that make the new processing lawful.

3.4 Which actors take part in the processing?

Apart from the essential actors referred to by the RGPD (the controller, the processor, the data subject and the DPO), other relevant actors may take part in the processing. It is important to determine who are these relevant actors, and the roles and responsibilities they have.

3.5 What are the processing operations?

Data can be processed automatically, manually or both; the processing can be carried out by the controller or delegated to a data processor; the processing can be done with the means of the controller or using external means (for example, processing done in the cloud).

The characteristics of the processing operation (such as the ones described above) have a deep impact on the risks associated with the data processing. For example, the use of computers and communication networks opens the door to a vast number of attacks, processing data in the cloud may lead to transfers of data outside the EU borders (which the RGPD limits).

3.6 Where does the processing take place?

Following WP29's approach, we do not consider data processing outside the EU to be a factor in determining whether a DPIA is required. However, if a DPIA is needed, international data transfers are an important point to consider because of the increased risks it brings.

Transferring personal data to a third country or international organization where the GDPR does not apply may result in diminished guarantees for the data subjects. For this reason, the GDPR restricts such data transfers, which can only be done if one of the following conditions applies:

- The European Commission considers that the third country, territory, sector of a country or international organization offers an adequate level of protection. In September 2019 these recognized countries are Andorra, Argentina, Canada (commercial organizations), United States (limited to the Privacy Shield), Guernsey, Isle of Man, Faroe Islands, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay.
- If the controller or the data processor provides the appropriate guarantees and the data subjects have enforceable rights and effective legal actions. Appropriate guarantees can be provided by:
    - A legally binding instrument that is enforceable between authorities or public bodies.
    - Binding corporate regulations, in accordance with article 47 of the GDPR.
    - Standard data protection clauses adopted by the Commission.
    - Standard data protection clauses adopted by a supervisory authority and approved by the Commission.
    - An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.
- Some of the derogations in article 49 apply.
    - The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
    - The transfer is necessary to execute a contract between the data subject and the controller.
    - The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request.

- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defense of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

4. Necessity and proportionality of the processing

Key points

- The processing must be effective in attaining its purpose.
- A processing operation is necessary when the purpose can not be attained in a less intrusive way.
- A processing operation is proportional when its benefits are superior to the potential harms.

In the description of the processing previously done, we have specified the purpose. Now, we have to assess the proportionality and the necessity of the processing in relation to its purpose.

We have to evaluate if the processing described in the previous section is effective in attaining its purpose, if there is an alternative that is less harmful to the rights and freedoms of people, and if the benefit obtained from the processing is superior to the potential harms that it may inflict on people.

To evaluate the necessity and the proportionality, we follow the basic principles that must govern any processing of personal data (article 5 RGPD). In particular, the principles of lawfulness, fairness, data minimization, storage limitation, and accuracy have a direct impact.

Apart from evaluating the previous principles, to establish the necessity and proportionality of the processing operation, we need to identify the risks for the rights and freedoms of people, the level of these risks and, propose measures to reduce them to a reasonable level. Section 6 discusses the risks from the point of view of information security; that is, the effects that a breach in the confidentiality, integrity or the availability of data may have on people. The analysis done in this section aims to determine the impact that treatment has on people in

the absence of security breaches. That is, the impact on people when the processing proceeds as planned.

4.1 Assessing the purpose of the processing

4.1.1 Processing for a purpose different than the one that motivated the collection

In general, the data should be processed exclusively for the purpose for which they were collected. If you want to process data for a different purpose, the new purpose must be compatible with the initial one, unless one of the following conditions applies[3]:

- The data subject has consented the processing for the new purpose.
- The processing is based on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in article 23(1):
  - National security.
  - Defense.
  - Public security.
  - The prevention, investigation, detection or prosecution of criminaloffenses or the execution of criminal penalties.
  - Other important objectives of general public interest.
  - The protection of judicial independence and judicial proceedings.
  - The prevention, investigation, detection, and prosecution of breaches of ethics for regulated professions.
  - The protection of the data subject or the rights and freedoms of others.
  - The enforcement of civil law claims.

4.1.2 Purpose compatibility

To evaluate whether a new purpose is compatible with the purpose that motivated the collection of data, the following aspects must be considered:

- The relation between the new purpose and the initial purpose.
- The context in which the data was collected. In particular, if the data subject can anticipate the new processing.
- The nature of the data. In particular, with regard to special categories (art. 9 RGPD) and data on sentences and criminal offenses (art. 10 RGPD).

[3] Article 6.4 RGPD.

- The potential consequences of the new processing.
- The existence of adequate guarantees.

As a general rule, if the new purpose is very different from the initial one and it is not a purpose that data subjects can anticipate, or if it can have an unjustified impact on them, it should be considered incompatible with the initial purpose.

The processing of personal data for the purpose of archiving in the public interest, for the purpose of scientific or historical research or for statistical purposes, is considered compatible with the initial purpose[4].

4.2 Lawfulness and fairness principles

4.2.1 Lawfulness

For a processing to be lawful, one of the following conditions must apply:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[4] Article 6.4 RGPD.

In addition, the data processing must be lawful in a broad sense. For example, it must not:

- Incur in an illegal act (civil or criminal).
- Violate copyright regulations.
- Violate contractual agreements.

When choosing the legal basis for the processing, the purpose and the context must be considered. No legal basis is better or more important than others. The processing may even be accommodated to multiple legal bases. In such a case, all suitable legal bases must be specified at the beginning.

Some of the legal bases have a specific purpose: to enter into a contract with the data subject, a legal obligation, to protect the vital interests of a person and the public interest. If the processing is done for any of these purposes, the appropriate legal basis is obvious.

When processing for other purposes, the legal basis may not be so obvious. In many cases, the controller may choose between legitimate interests and consent. If legitimate interest is chosen, the controller keeps close control over the processing; but it becomes necessary to show that the legitimate interest of the controller is not offset by rights of the data subject. If consent is used as a legal basis, data subjects are given full control over the use of their data (including the possibility of withdrawing their consent; thus, forcing the controller to stop processing their data).

It is convenient to make the right choice from the beginning. If we discover, after the processing has been initiated, that the legal basis is inadequate, it may be difficult to change it. Even if it was possible to apply another basis, the data subjects may not understand such change.

Example

An organization decides to process personal data using consent as legal basis. After collecting the consent of the data subjects and initiating the processing, there is a person who wishes to withdraw the consent given. The organization, which wishes to continue processing the data, decides to continue based on legitimate interest.

In this case, by choosing consent as legal basis, the controller made data subjects believe that they were in control of the processing of their data when it was not. The organization should have made it clear from the beginning that the treatment was based on the legitimate interest. At this point, to honor the expectations of data subjects, it should stop processing data of people that have withdrawn consent.

4.2.1.1 Child data processing

Children need special protection with respect to the processing of their data, because they may not be aware of the risks involved.

When the processing is related to the direct provision of services of the information society to children and the legal basis is consent, the RGPD establishes a minimum age of 16 years for the consent to be valid. Under the age of 16, consent must be given or authorized by the holder of the custody. Member states can reduce the minimum age for consent, but it cannot be less than 13 years.

In the Spanish case, the minimum age for consent is 14 years. The following table shows the minimum age for consent in relation to the direct offer of services of the information society:

Minimum age for consent (July 2019)[5]

13 years	14 years	15 years	16 years
Belgium	Austria	Czech Republic	Germany
Denmark	Bulgaria	France	Croatia
Estonia	Spain		Slovakia
Finland	Italy		Slovenia
Latvia	Lithuania		Greece
Malta	Cyprus		Netherlands
Portugal			Hungary
United Kingdom			Ireland
Sweden			Luxembourg
			Poland
			Romania

[5] www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751

4.2.1.2 Processing special categories

Special category data are more sensitive and, therefore, need more protection. When these data are processed, apart from determining a legal basis for the processing, we need to determine one of the conditions of article 9 that allows the processing:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where a Union or Member State law prohibits it.
- Processing is necessary for the purposes of carrying out the obligations in the field of employment, social security, and social protection law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health.
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The legal basis used for the processing does not restrict the legal bases available for the processing of special categories of data. For example, the use of consent as a legal basis does not imply the use of explicit consent as a basis for processing special category data. However, in some cases, there is a clear link between both. For example, if the legal basis is the vital interest, vital interest is likely to be the basis for the processing of special categories of data.

4.2.1.3 Processing data related to criminal convictions and offenses

Although not a special category of data, the data on convictions or criminal offenses also enjoy special protection. The processing of these data is only allowed under the supervision of the public authorities or when authorized by the right of the union or the member state. In addition, when the processing involves comprehensive records of criminal convictions, these must be kept under the control of the authority.

4.2.1.4 Validity of consent

For consent to be valid the following conditions must be met:

- The controller must be able to show that consent has been collected.
- The request for consent must be intelligible, easily accessible and use a clear language.
- The execution of a contract cannot be subject to receiving consent to process personal data that are not necessary to execute the contract.
- The data subjects have been informed of the possibility of withdrawing their consent at any time.

The withdrawal of consent does not affect the validity of any processing done before the withdrawal.

4.2.2 Fairness

Processing is fair if the use of data it makes (in relation to the purpose of the processing) can be anticipated by the data subjects and does not result in adverse consequences for the data subjects that are not justifiable.

4.3 Minimization principle

The principle of data minimization determines that the data must be adequate (sufficient to comply with the purpose of the processing), relevant (they are related to the purpose of the processing) and limited to what is strictly necessary to fulfill the purpose of the processing.

In order to comply with the principle of minimization, it is necessary to identify the minimum information necessary to meet the purpose of processing. Such information must be collected and nothing more.

The level of detail of data is also important to comply with the minimization principle. Data must have a level of detail that is relevant to the purpose of the processing.

The data that is relevant may vary from data subject to data subject. In this case, it is necessary to adjust the data processed to those relevant in each case.

It is necessary to periodically check that stored data remain relevant and adequate for the purpose of the processing and to erase any data that is not.

With respect to data adequacy, it must be guaranteed that they are useful to achieve the purpose of the processing. We should not any data if they are insufficient or incomplete for the intended purpose.

4.4 Storage limitation principle

Personal data should only be kept for as long as it is necessary to meet the purpose of the processing. Ensuring that personal data are deleted when they are no longer necessary reduces the risk of data becoming irrelevant, excessive or inaccurate.

Following article 30.1, when possible, it is necessary to establish and document standard retention periods for different types of data. Additionally, the organization must have the necessary procedures to review and make effective these retention periods.

The controller is responsible for setting the retention period, in accordance with the needs of the processing. Data must not be kept indefinitely, just in case they become necessary in the future.

Data can be kept indefinitely for the purpose of archiving in the public interest, for the purpose of scientific or historical research, or for statistical purposes. In these cases, it is necessary to deploy any technical and organizational measures required to guarantee the principle of minimization. Techniques such as anonymization or pseudonymization of data may be useful in this context.

4.5 Accuracy principle

The processing of inaccurate data can have a negative impact on data subjects. The accuracy principle requires data to be accurate and demands the controller to establish appropriate measures to ensure any inaccuracy is amended without delay.

4.6 Risks related to the processing

Any data processing may have negative effects on the rights and freedoms of data subjects. To mitigate them, the GDPR proposes a risk-based approach. The measures to protect the

rights and freedoms of people adopted must be proportional to the risk associated with the processing.

Typically, risk assessment is done from the point of view of the organization that processes the data. That is, it focuses on the negative effects on the controller. The

RGPD changes this point of view and seeks to evaluate the risk of the processing on data subjects.

Information security is a key point in risk assessments. That is, we normally evaluate the potential negative effects of a breach in the security of processing. However, processing can affect the rights and freedoms of people, even in absence of security breaches. For example, a processing operation can be discriminatory in itself or may favor the emergence of discriminatory practices. This section focuses on this last vision: assessing the risk of processing in itself.

Comment

Any data processing, whether personal or not, can have negative effects on people. In a DPIA, we are only interested in the effects derived from the use of personal data.

For example, a processing that is based on aggregate (hence non-personal) data can have a significant effect on people. For as long as the impact is not related to the use of personal data, we need not take it into consideration.

The negative effects of processing on data subjects are specific to each processing operation. We list some examples below. This list is by no means comprehensive and it is the responsibility of the controller to make sure that all potential negative effects have been identified.

- Waste of time.
- Anger.
- Increase in costs.
- Lack of understanding.
- Stress.
- Inability to access services or other opportunities.
- Discrimination.
- Theft of identity and other frauds.
- Economic losses.
- Psychological damages.
- Damages for reputation.

- Physical injuries.
- Health affectation.
- Loss of work.
- Serious physical or psychological damages.

To determine the effects that a processing operation may have on data subjects, we have to consider some characteristics, such as:

- The type of personal data. The processing of special categories of data, such as racial or ethnic origin, medical data or data on political preferences, are clear indicators of potential negative effects on the rights and freedoms of individuals. However, it should be noted that other types of data that are not part of the special categories can also have an important impact. For example, locations, financial information, etc.
- The degree of sensitivity of the processing. Beyond the type of data treated, the type of processing can also point to potential impacts. For example, when the processing aims at monitoring people.
- The amount of personal data processed on each data subject. The more data, the greater the potential negative effects on people.
- The activity of the controller. For example, if the activity of the controller has to do with health or finance, the potential impact is likely to be high.
- The characteristics of the data subjects. If the data subjects are part of a group with special needs (for example, children or public authorities), special care must be taken when determining the potential effects of the processing.

According to the GDPR, when conducting a DPIA, it is convenient to gather the opinion of the data subjects about the processing. Since the risk assessment in a DPIA focuses on data subjects (rather than on the organization), it is interesting to gather their opinion about the risk of the processing.

4.6.1 Impact

Once the potential negative effects have been identified, it is necessary to determine their impact. We consider four levels of impact: low, medium, high and very high.

Impact	Description
Low	Data subjects may suffer some minor inconveniences, which they can overcome without problems (for example, loss of time, anger, etc.)
Medium	Data subjects can suffer important inconveniences, which can be overcome with some difficulties (for example, increased costs, lack of understanding, stress, physical harm, the impossibility of accessing a service, etc.)
High	Data subjects may suffer significant consequences, which may be overcome with major difficulties (for example, discrimination, theft of identity, economic loss, psychological damage, damage to reputation, physical harm, worsening of health, job loss, etc.).
Very high	Data subjects can suffer serious consequences that cannot be overcome (for example, severe or physical psychological damage, death, etc.)

Same as before, the controller has the responsibility for evaluating the impact.

4.6.2 Threats and probability

Although processing may have negative effects on data subjects, these effects need not always materialize. To evaluate the risk of a potential negative effect, it is necessary to estimate its probability.

We consider three levels of probability:

- Although processing may have negative effects on data subjects, these effects need not always materialize. To evaluate the risk of a potential negative effect, it is necessary to estimate its probability.
- We consider three levels of probability.

This probability can be estimated directly. However, without an analysis of the conditions in which the impact is materialized, the estimate is likely to be inaccurate. For this reason, we will estimate the probability in terms of threats.

A threat is any circumstance that has the potential to materialize one of the negative effects of the processing. Once threats have been identified, it is necessary to determine their probability. The probability of a threat remains a subjective estimate; however, threats being more specific than negative effects, their probability is easier to estimate.

4.6.3 Risk estimation

The risk of a negative effect is computed from the impact and the probability. Since we have done a qualitative estimation of the latter, the risk estimation will also be qualitative.

When calculating the risk in a DPIA, it is essential to focus on the negative effects of the processing on the data subjects. From the point of view of the controller, a very high impact on a data subject could be acceptable, if the probability is small; the controller may decide to assume the cost associated with such an event. However, the point of view of data subjects may be different, since they receive the impact. In general, data subjects may be less likely to accept high impacts even if their probability is small since recovering from these impacts could be very difficult or even impossible.

We propose the following risk calculation table. In accordance with the previous discussion, if the impact is very high, the risk will be high regardless of the probability.

	Impact			
Probability	Low	Medium	High	Very high
High	Medium risk	High risk	High risk	High risk
Medium	Low Risk	Medium risk	High risk	High risk
Low	Low Risk	Low Risk	Medium risk	High risk

4.6.4 Risk reduction

Except when the risk is already low, we should strive to reduce it. This is particularly necessary for high or very high risks. If it is not possible to reduce a high risk, we must consult the data protection authority about the suitability of the processing before it starts.

The appropriate measures to reduce risk depend to a great extent on the processing and it is the controller who has to determine them. Some measures are:

- To avoid collecting certain types of data.
- To reduce the scope of processing.
- To train staff to avoid inappropriate usage of the data.
- To anonymize or pseudonymize the data.
- To restrict access to the data.

For information security risks, it is usual to calculate an initial risk (without security controls) and a residual risk (with the security controls implemented to reduce risk). This is possible because the security controls do not alter the essence of the processing. However, for the risk associated with the processing in itself, the measures to reduce it are, basically, modifications to the processing operation. For this reason, it is necessary to update previous sections of the DPIA with the changes made to the processing operation and, then, recalculate the risk. In this sense, the DPIA is not a linear task.

Example

A company launches a selection process for recruiting staff. The purpose of this selection process is to choose the most suitable person for a specific position.

In a broad sense, any selection process discriminates. However, we want this discrimination to be based on the capacities of people, rather than on spurious reasons.

To contact the candidates, data about their address may be collected. An evaluator with access to such information may exclude candidates who live in marginal zones. If we estimate the impact as high and the probability as medium, the resulting risk is high. Therefore, we need to implement measures to reduce it.

As the address of candidates is not necessary to evaluate their capabilities for a job, we can reduce the risk by not making it available to evaluators. Such a measure does not only reduce the risk of discrimination against people but also helps the company to get the most suitable person for the job.

4.7 Necessity and proportionality

Once the principles of data protection have been evaluated and the risks for the rights and freedoms of data subjects assessed, the controller has the necessary information to evaluate the necessity and proportionality of the processing.

The processing only makes sense if it achieves its purpose. Therefore, justifying the effectiveness of the processing is the first step to justify its necessity. Additionally, to justify the necessity, we need to show that there is no other processing that achieves the purpose and is less harmful to the rights and freedoms of data subjects.

To justify the proportionality of the processing, we have to show that the benefits of the processing are superior to potential harms that data subjects may face. In this task, it is advisable to take into account the risk analysis made in the previous section.

4.8 Data subjects' opinion

The controller should gather the opinion of data subjects about the processing operation. The necessity and the proportionality of the processing is a particularly interesting topic to gather the data subjects' opinion about. When gathering such opinion is deemed inappropriate, the controller must document the reason why. For example, because it has a disproportionate cost or because it can jeopardize the confidentiality of a business plan.

5. Data subject rights

Key points

- The GDPR establishes a series of rights to allow data subjects to know and intervene in the processing of their data.
- When assessing the impact of the processing, we must ensure that data subjects can exercise these rights.

The fundamental principles referred to in Article 5 of the Regulation are reflected in a series of rights set forth in Chapter 3: transparency, information, access to personal data, rectification, erasure, restriction of processing and opposition.

These rights give data subjects the ability to know and to intervene in the processing. Transparency and the right to information are necessary for data subjects to be aware of how their data is processed. The rights of access, rectification, and erasure allow the interested parties to control their data. The rights to restriction of processing and to object give data subjects control over the processing.

It is essential to ensure that data subjects can exercise their rights. The goal of this section is to evaluate the mechanisms established for it.

5.1 Transparency

Transparency as a transversal property that must be present anytime a communication to the data subjects is done. More specifically, transparency requires any communication with the data subjects to be concise, intelligible, easily accessible, and to use a clear and simple language. Especially when this communication is addressed to a child.

It also requires the controller to act on the requests of data subjects within a reasonable time. In particular, the regulation establishes a period of one month, which can be extended (after

notification within the first month) in two additional months, if justified by the complexity or number of applications.

Finally, the controller is required to inform without undue delay about the decision of not acting on a data subject request, about the reasons, and about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

In the course of a request, if the controller has doubts about the identity of the data subject, the controller may request additional information necessary to confirm the identity.

5.2 Right to be informed

Data subjects have the right to be informed about the collection and subsequent processing of their data. This is an essential right; without this information, the other rights cannot be made effective.

According to the right to be informed, data subjects must receive the following information:

- The identity and contact details of the controller.
- Contact data of the data protection delegate (if any).
- The purpose of the processing.
- The legal basis of the processing.
- The legitimate interest of the controller, if this is the legal basis of the processing.
- The recipients or categories of recipients of the data.
- The period of retention of the data or the criterion used to determine it.
- The intention to transfer the data outside the EU, if applicable.
- The decision of the European Commission regarding the sufficiency of the security offered by the recipient country or organization.

In addition, to ensure that the interested parties know their rights and know how to exercise them, the controller must inform them about them:

- Right to access the data.
- Right to rectify and suppress.
- Right to limit the processing.
- Right to object to the processing.
- Right to data portability.
- Right to revoke consent (if this is the legal basis of the processing).
- Right to file a complaint with a supervisory authority.

And, likewise:

- That the communication of the data is a legal or contractual requirement, if applicable.
- The existence of automated decisions.

If data have been collected from a third party, data subjects must be informed of its origin.

When data is collected directly from data subjects, the previous information must be provided at the time of data collection. When data is not collected directly from the interested parties, it is necessary to inform:

- Within a reasonable period after obtaining the personal data, but at the latest within one month.
- If the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject.
- If a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

There are some exemptions to the obligation to inform, which depend on how the data has been collected:

- If the data were obtained directly from the data subject, there is no obligation to inform you if you already have the information.
- If the data were not obtained directly from the data subject, there is no obligation to inform you if one of the following conditions applies: the data subject already has this information.
- The communication is impossible or requires a disproportionate effort, it is regulated by an EU or member state rules, or the information is confidential on the basis of professional secrecy.

If the data subject is not informed, it is necessary to justify it.

5.3 Right to access

Data subjects have the right to obtain from the controller the confirmation that their data are being processed and, in that case, the right to access the personal data and the following information:

- Purpose of the processing.
- Data categories treated.
- Recipients of the data.
- Period of retention of the data.

- Right to rectify and to erase the data.
- Right to restrict and to oppose to the processing.
- Right to lodge a complaint with a supervisory authority.
- Source of the data, if they were not collected from the data subject.
- Existence of automated decisions, if applicable.
- Guarantees on the transfer of data outside the EU, where appropriate.

The controller must also make sure that data subjects can make effective their right of access.

How is a valid application recognized?

The Regulation does not specify how access requests should be made. They can be addressed to any employee, by any means and do not require any phrase like "request for the right of access". Thus, it is necessary to make sure that the personnel that interacts with data subjects can identify access requests.

Is a standard procedure required?

It is advisable to establish a standard procedure to make the requests. This facilitates things both to the controller and to data subjects. However, requests remain valid even if they do not use such a procedure.

Transparency requirements apply to the right to Access:

- The information must be concise, intelligible, easily accessible and must use a clear and simple language.
- Requests must be processed within one month.
- If the complexity or the number of requests require it, this term can be extended by two months, after notifying the data subject.
- The controller may ask for the information necessary to confirm the identity of the person making the request.
- Requests must be free, except when they are unfounded or excessive.

5.4 Right to rectification

Data subjects have the right to rectify personal information that is not accurate. The exercise of this right is more involved because the accuracy of the data may also be a matter of personal perception.

After receiving a request, the controller must take the necessary steps to verify if data are accurate and, if necessary, rectify them. During the time it takes for the controller to check the accuracy of the data, data subjects have the right to limit processing.

If the controller concludes that the data is already accurate and, therefore, that there is no need to rectify it, the interested party must be informed. It is necessary to explain the decision and inform of the possibility of lodging a complaint with a supervisory authority. According to article 19, if the controller has shared the data, appropriate steps must be taken to inform recipients about the request for rectification (considering the costs and technology available).

Según el artículo 19, si el responsable ha compartido los datos, debe tomar las medidas adecuadas (teniendo en cuenta los costes y la tecnología disponible) para informar a las personas destinatarias sobre la petición de rectificación.

5.5 Right to erasure

A data subject has the right to have data erased in the following cases:

- Data are no longer necessary in relation to the purpose for which they were collected.
- The data subject withdraws their consent and there is no other legal basis for the processing.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The data have been processed unlawfully.
- The data must be erased in accordance with a legal obligation to which the controller is subject.
- The data is used to offer information society services to children.

If the controller has shared the data, it is necessary to take the appropriate steps to inform the recipients about the request (considering the costs and technology available).

The right to erasure does not apply when the processing is necessary:

- For exercising the right of freedom of expression and information.
- For compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For reasons of public interest in the area of public health.
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, if compliance with these purposes is affected by the erasure of the data.
- For the establishment, exercise or defense of legal claims.

5.6 Right to limit processing

Data subjects have the right to limit the processing of their data, in the following cases:

- The data subject has requested the rectification of data and the controller is checking their accuracy.
- The processing is unlawful.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
- The data subject has objected to processing but the controller is checking whether the legitimate grounds of the controller override those of the data subject.

The notion of processing is very general: it includes, among others, the collection, analysis, dissemination, and deletion of data. It is important to consider all forms of processing when limiting it.

If the controller has shared the data, it is necessary to take the appropriate steps to inform the recipients about the request (considering the costs and technology available).

5.7 Right to data portability

According to article 20, data subjects have the right to request the data they have provided to the controller in the following cases:

- If the processing is based on the consent or is necessary to execute a contract or to apply pre-contractual measures.
- The processing is done through automated means.

The right to data portability is not limited to the data that data subjects have explicitly given; it also affects the data collected from the observation of data subjects. For example, the search log in a search engine or the location information that an app has collected from a GPS. Data must be transmitted in a common format.

The right to data portability should not adversely affect other people. In particular:

- If the personal data contain information related to a third person, it is necessary to evaluate if the rights and freedoms of the latter may be affected.
- If the data relate to several people (for example, a shared bank account), we must seek the consensus of all those interested.

5.8 Right to object

According to article 21, data subjects have the right to object to the processing of their data when the processing is based on:

- Public interest or the exercise of public powers conferred on the person in charge of the treatment.
- The legitimate interest of the controller. In this case, the controller must stop the processing, unless the legitimate reasons prevail over the rights of the data subject.

The Regulations considers the following cases:

- Opposition to processing for marketing purposes. In this case, the controller must stop the processing without exception.
- Opposition to processing for scientific or historical research, or for statistical purposes. In this case, the controller may continue the processing if it is justified by the public interest.

5.9 Right not to be subject to automatic decisions

According to article 22, data subjects have the right not to be subject to automated decisions (including profiling), if they have legal effects or have another significant effect, unless:

- It is necessary for entering into, or performance of, a contract between the data subject and a data controller.
- It is authorized by a UE or a member state law.
- It is based on the explicit consent of the data subject.

The data subject has the right to obtain human intervention, to express her or his point of view, and to challenge the decision.

Automated decisions can only make use of special categories of data if the data subject has given explicit consent, or if the processing is done to protect the vital interests of the data subject or another person.

6. Information security risks

According to the GDPR, the level of security must be adequate to the risk to the rights and freedoms of data subjects. In section 4.6, we evaluated the risk of the processing in itself. In this section, we evaluate the risk from the point of view of information security; that is, the risk associated to a breach in the confidentiality, integrity or availability of the data.

We follow the process described in section 4.6: based on the description of the processing previously done, we evaluate the impact and the probability of a breach in one of the security properties. First, we compute the initial risk of the processing. If this risk is too large, we must apply security controls (protection measures) to reduce it. These controls may seek to reduce the impact or the likelihood of security breaches. Finally, we compute the residual risk; that is, the risk after the implementation of the selected security controls.

The GDPR cites the following protection measures that may be considered (among others)[6]:

- Pseudonymization and encryption of data.
- Measures to guarantee the confidentiality, integrity, availability and resilience of treatment systems and services.
- Measures to recover the availability and access to personal data in a suitable time, in case of a security incident.
- A continuous process of testing and evaluation of the effectiveness of the measures.

Regarding the risk analysis methodology, there are those that have a broad recognition, such as: ISO 27005:2013, OCTAVE, NIST SP 800-30 and Magerit. Now, taking a risk analysis using these methodologies can be a complex process.

In order to make the risk assessment more affordable to organizations with limited resources (e.g. small and medium size enterprises), this guide proposes a simplified risk analysis procedure. However, if the organization has enough resources to employ one of the methodologies previously mentioned, it is advisable to do so.

Regardless of the risk assessment methodology used, we must not forget that the focus of this risk assessment must be set on the data subjects (rather than on the organization).

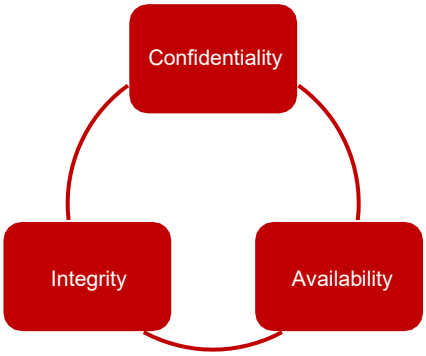
6.1 Brief introduction of information security

Information security encompasses the set of measures (technical, organizational, etc.) that are taken to protect the information that is processed against unauthorized access, disclosure, modification, and destruction.

The CIA triangle is a well-known information security model. It refers to the three essential properties of information security: confidentiality, integrity, and availability.

[6] RGPD, article 32.1.

- Confidentiality. Only persons, entities or processes that have been previously authorized should have access to the information.
- Integrity. Only persons, entities or processes that have been previously authorized can modify the information.
- Availability. The information must be available when an authorized person, entity or process requests it.



There are information security models that complement the previous three properties. For example, by adding authenticity and traceability. In our risk estimation, we focus on three basic properties.

6.2 Impact

The first step to assess the risk is to determine the impact that the loss of confidentiality, integrity or availability can cause on data subjects. Recall that our risk assessment focuses on people rather than on the organization.

To determine the impact, we should consider all possible situations that lead to a loss of confidentiality, integrity, and availability. To facilitate this task, we list some scenarios in which some of these properties are lost.

Scenarios involving a loss of confidentiality:

- The loss or theft of a computer that contains personal data.
- To send by mistake an email containing personal data to an unauthorized person.
- Unauthorized access to a person's account.
- Configuration error in a web that exposes the personal data of its users.
- To steal information from the facilities of the controller.
- An employee access customers' information for illegitimate purposes.

Scenarios involving a loss of integrity:

- An employee modifies the data of a client by mistake.
- An error in the communications network alters the data while in transit.
- A company maintains several copies of the data, but a change in one of the copies does not propagate to the others.
- Some information is lost due to a failure in one of the IT systems.

Scenarios involving a loss of availability:

- A file is corrupted or deleted and there is no backup.
- A paper document is lost, and there are no copies of it.
- A data access service is not available.

Following section 6.2, we use four different levels to measure the impact on data subjects of a breach in data security: low, medium, high or very high. To determine the impact level, it is necessary to consider the characteristics of the processing. The following situations increase the risk:

- Processing of special categories or other particularly sensitive data (financial information, locations, etc.).
- Monitoring of people.
- Processing data related to groups with special needs (children, authorities, etc.).
- The processing of large amounts of data of each data subject.

As a result, we will have an impact on each of the security properties: one for loss of confidentiality, one for the loss of integrity and one for the loss of availability. We also calculate the overall impact of the processing system, as the maximum of the previous impacts.

6.3 Initial probability

To keep the analysis simple, the estimation of the probability will not be based on an inventory of the system assets, vulnerabilities, and threats. Our estimate is based on the identification of some characteristics of the system that make it more prone to suffer from attacks. These characteristics can be classified into different categories: hardware and software, processing operations, people involved in the processing and other features.

Hardware and software

Is the processing system connected to external systems?

The connection with external systems increases exposure to threats. For example, information may be captured or maliciously modified while in transit, security breaches in the external system may put the security of the data at risk, etc.

Examples

- The processing system of a hospital is connected to the systems of several private insurance companies. A security breach in the systems of the insurance companies may put the data processed by the hospital at risk.
- Workstations that are part of the processing system have access to the Internet.

Is any part of the processing done through the internet?

Interaction with data subjects through the Internet exposes the processing system to external threats, such as phishing, SQL injection, man-in-the-middle attacks, DoS and XSS. These threats may compromise the processing system and the security of the data (confidentiality, integrity, and availability).

Allowing the personnel of the organization to access the processing system over the Internet increases exposure to external attacks and, also, increases the probability of workers misusing the information (accidentally or intentionally).

Examples:

- Online stores, online banking, etc**.**
- The use of e-mail as part of the processing system introduces several threats. First, many times, e-mails are not encrypted, which may put the confidentiality of the data at risk. Additionally, the use of e-mail increases the probability of suffering e-mail phishing and spoofing attacks.
- The administrators of the processing system can do maintenance tasks over the internet.
- The access to the processing system from a public place (e.g. public transportation, bar, etc.) may put the confidentiality of the data at risk**.**

Is there a failure to follow a relevant good practices document in the design and the configuration of the processing system?

If the processing system is not well designed or the elements that compose it are not properly configured, data security risks increase. There are many good-practices guides dealing with different security-related topics (networks, computers, etc.).

Examples

- The design of the network must follow a good-practices document that includes elements such as firewalls, network segmentation, and VPN usage.
- The configuration of the computers used must follow a good practices document. The number of aspects that need to be considered when configuring a computer is so large that following a document is essential. For instance, user privileges, antivirus, strong passwords, system lock after an inactivity periods are just a few topics.
- The processing system should be sized considering the computing, communication and storage needs that are anticipated. Additionally, it must be provided with enough staff.
- The configuration of the software used must follow a good-practices document. For example, securing a web server, etc.
- The development methodology must take the security of the data into account throughout the entire life cycle of the application.

Is there a lack of following a relevant good practices document in the maintenance, monitorization and response to incidents?

It is essential to maintain and monitor the system properly. Maintenance must be made both for devices and software. Monitoring the system allows incidents to be analyzed once they have happened. Monitoring may also be used to detect suspicious behavior to prevent security incidents from happening, and to improve the reaction time, thus, reducing their impact.

Examples

- Failure to apply operating system security updates can lead to new attack vectors.
- The lack of regular backups can lead to the loss of information in case of an incident.

Is there a lack of physical security in the processing facilities?

The physical security of the processing facilities is essential. Without it, the security of the processing system (electronic or not) cannot be guaranteed.

Examples

- If the data center lacks appropriate access controls, we cannot prevent unauthorized people from entering it.
- Due to space limitations of the physical archiving facilities, documents are being kept in other places that do not offer the necessary security guarantees.
- The data center is not safe against natural and industrial accidents (for example, electrical failures, floods).
- A cloud service is used without having guarantees that the provider facilities are sufficiently protected.

Use of the processing system

Is there a lack of clarity in the roles and responsibilities of the employees?

A lack of clarity in the definition of roles and responsibilities can lead to uncontrolled use of data (either accidental or intentional).

Examples

- A worker from a bank office should only consult the data of their clients.
- The personnel of the organization is responsible for destroying the information safely when no longer required.
- The personnel of the organization is responsible for maintaining the security of data when they communicate them to another person or organization.

Is there a lack of clarity in the definition of acceptable uses of the processing system??

When acceptable uses of the processing system are not clearly defined, the risk of misuse is increased.

Examples

- The installation of file-sharing software can lead to involuntary file sharing.
- The installation of software by regular users (that is, users other than the system administrators) can lead to insecure configuration and poor maintenance.
- Visiting malicious webpages can be a source of malware and data theft.

Can the personnel connect external devices to the processing system?

The connection of devices external to the treatment system is a gateway to the entry of malware, the introduction of vulnerabilities, etc. In addition, it also makes it easier for personnel to extract information.

Examples

- An employee connects a phone or a memory stick to the USB ports of the computer.
- An employee uses her device to perform processing tasks (BYOD).

Is there a lack of adequate procedures for registering and supervising the processing activities?

The lack of a log of the activities (log file) can increase the bad practices of the personnel and, at the same time, hinders the investigation of the incidents once they have taken place.

Examples

- Patient records can be queried without access to the data being logged.
- Despite a log of the data processing activities carried out by each employee is generated, it is not monitored.
- Employees can access the data center without leaving a trail.

People

Does the personnel have permissions that are not necessary for the tasks assigned to them?

The larger the number of people with access to some data, the greater the likelihood of abuse. To avoid this, it is essential to control the accesses of the personnel to the system and authorizes only those that are strictly necessary to perform their duties.

Examples

- Access to a patient's clinical history should be limited to the professionals who treat her.

Has some part of the processing been outsourced to a processor?

Outsourcing the processing (or part of it) to a processor results in a loss of control over the data. It is the responsibility of the controller to choose a processor that offers the necessary level of security and defines the responsibilities of the processor clearly.

Examples

- A cloud is used to perform part of the processing.
- The controller lacks the knowledge to perform some data analysis and outsources.

Does the personnel lack basic capabilities, attitude or knowledge regarding the proper use of the system and data security?

The personnel of an organization is an essential part of any data processing performed by the organization. Personnel must have the necessary qualifications and attitude towards the job. A lack of knowledge by the personnel about the proper use of the system, about information security or about the obligations and limitations imposed by the RGPD can lead to bad practices that may put the security of the data at risk.

Examples

- A person that lacks basic knowledge about data security is more prone to act carelessly. For instance, by keeping sensitive data in a laptop device that is more prone to a thief and is unlikely to have a backup copy; or by following the instructions in a phishing email that seeks to gain access into the processing system.

Other characteristics

Has the organization or other organizations in the sector been attacked recently?

The fact that an organization has suffered from previous attacks may indicate that attackers see the organization as an interesting target.

Additionally, recent attacks suffered by other organizations in the same sector should also be a warning sign of potential attacks. Indeed, many attacks are conducted in campaigns. The reason is that when launching a new malware, attackers seek the greatest impact before people can react to it.

Have people complained about the stability or the security of the processing system?

The presence of bugs in the processing system increases the likelihood of losing data, of altering data and, even, of suffering an attack. In the same way, notifications about potential security issues in the processing system should also be taken seriously.

Are data of special interest or data of many users being processed?

The presence of large amounts of data and the presence of especially sensitive data may be an extra motivation for attackers.

Ejemplo

- Ransomware encrypts the files in a system and then asks for a ransom to recover them. The greater the importance of the data, the more likely the attackers will get the ransom.
- An online store may keep the credit card information about their clients. Gaining access to such data may be an extra motivation for attackers.

Each affirmative answer to the previous questions indicates an increase in the probability of suffering data security incidents. To estimate the initial probability (without security controls), we count the number of affirmative answers and apply the following table:

Afirmative answers	**Initial probability**
0 - 4	Low
5 – 9	Medium
10 - 15	High

6.4 Initial risk

Once we have estimated the impact and the initial probability, we can compute the initial risk (that is, the risk without additional security controls). We use the same table that was used in section 4.6.

	Impact			
Probability	Low	Medio	Alto	Muy alto
High	Medium risk	Riesgo alto	Riesgo alto	Riesgo alto
Medium	Low risk	Riesgo medio	Riesgo alto	Riesgo alto
Low	Low risk	Riesgo bajo	Riesgo medio	Riesgo alto

As a result of this section, we get the initial risk for each of the security properties (confidentiality, integrity, availability), as well as a global initial risk (the maximum of the previous risks).

6.5 Security controls

Once the initial risk has been calculated, it is necessary to determine which controls (measures to reduce risk) must be applied. The security controls to be applied should be proportional to the risk. If the initial risk is high, the use of security controls to reduce it is mandatory. However, it is advisable to apply controls according even when the risk is lower.

Security controls act on the risk in various ways: by preventing security incidents from happening, by reducing the impact of incidents, by facilitating recovery, etc.

To plan the security controls, we need to use one of the standard lists of controls available. Otherwise, there is a high risk of missing important controls. There are many such lists. Although any (of the many standard lists available) should be fine, in this guide we use the ISO 27002. In the trailing part of the section, we list the ISO 27002 security controls. Note that, due to regulatory requirements in Spain, the Catalan version of the guide uses the controls defined in the "national security outline" (in catalan, esquema nacional de seguretat).

In the following table, we provide some guidance with respect to the effect that groups of security controls in the ISO 27002 have on the questions that we have used to estimate the probability. To reduce the probability of negative effects, we must apply security controls that target those questions with an affirmative response. The more thoroughly the controls deal with the issue pointed out in a question, the less likely the negative impact will be materialized. If we judge that, after applying the controls, the probability of a negative effect is negligible, we can change the response to the associated question from 1 to 0.

Control	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
A.5.1			x	x											
A.6.1			x	x		x				x					
A.6.2		x						x							
A.7.1						x						x			
A.7.2						x	x					x			
A.7.3						x									
A.8.1						x	x								
A.8.2						x	x			x					
A.8.3					x		x		x						
A.9.1					x	x			x	x					
A.9.2									x	x					
A.9.3										x					
A.9.4				x					x	x					
A.10.1			x	x											
A.11.1				x	x										
A.11.2															
A.12.1			x	x											
A.12.2	x	x													
A.12.3				x	x										
A.12.4				x											
A.12.5							x		x						
A.12.6				x											

Control	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
A.12.7									x						
A.13.1	x	x									x				
A.13.2	x	x									x				
A.14.1			x												
A.14.2			x												
A.14.3			x												
A.15.1										x					
A.15.2										x					
A.16.1			x	x											
A.17.1			x	x											
A.17.2			x	x											
A.18.1			x	x											
A.18.2			x	x											
A.5.1			x	x											
A.6.1			x	x		x				x					
A.6.2		x						x							
A.7.1						x						x			
A.7.2						x	x					x			
A.7.3						x									
A.8.1						x	x								
A.8.2						x	x			x					
A.8.3					x		x		x						
A.9.1					x	x			x	x					
A.9.2									x	x					
A.9.3										x					
A.9.4				x					x	x					
A.10.1			x	x											
A.11.1				x	x										
A.11.2															
A.12.1			x	x											
A.12.2	x	x													
A.12.3				x	x										
A.12.4				x											
A.12.5							x		x						
A.12.6				x											

Control	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
A.12.7									x						
A.13.1	x	x									x				
A.13.2	x	x									x				
A.14.1			x												
A.14.2			x												
A.14.3			x												
A.15.1										x					
A.15.2										x					
A.16.1			x	x											
A.17.1			x	x											
A.17.2			x	x											
A.18.1			x	x											

In general, it is difficult to reduce the impact of a violation in one of the security properties. In other words, although controls may reduce the probability of a confidentiality loss, the impact is likely to remain unaltered. However, in some cases, controls may also reduce the impact. For example, having a backup of storage devices may reduce the impact of a faulty device. It is the controller who must describe and justify any reduction in the impact that results from the use of security controls.

A.5. Information security policies

A.5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

A.5.1.1 Policies for information security

The organization should define a set of policies for information security, which must be approved by management, published, and communicated to employees and external parties.

A.5.1.2 Review for policies for information security

The policies for information security must be reviewed periodically to make sure that they remain appropriate, especially in the case of significant changes in the system.

A.6 Organization of information security

A.6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1 Information security roles and responsibilities

Security responsibilities must be defined and assigned.

A.6.1.2 Segregation of duties

Duties must be segregated to limit the risk of misuse of the assets.

A.6.1.3 Contact with authorities

There should be a clear description of the authorities that need to be contacted in case of information security incidents.

A.6.1.4 Contact with special interest groups

Contact with information security professionals must be kept (e.g. to get security advice, to improve the security of the system, etc.)

A.6.1.5 Information security

In project management Information security must be present in all the phases of a project.

A.6.2 Mobile devices and teleworking

A.6.2.1 Mobile device policy

The use of mobile devices introduces many risks (e.g. they may be lost or theft, users may install many applications, etc.). A policy regarding the use of mobile devices must be defined.

A.6.2.2 Teleworking

A policy must be defined to guarantee the security of the information processed when teleworking.

A.7 Human resource security

A.7.1 Prior to employment

A.7.1.1 Screening

Background verifications on candidates should be done in accordance with the business requirements and the perceived information security risks.

A.7.1.2 Terms and conditions of employment

The security responsibilities of employees should be stated in the contractual agreement.

A.7.2 During employment

A.7.2.1 Management responsibilities

Management must require all employees to follow the security policies and procedures established by the organization.

A.7.2.2 Information security awareness and training

All personnel of the organization should receive periodic training on the policies and procedures relevant to their tasks.

A.7.2.3 Disciplinary process

A disciplinary process that targets employees that have committed information security breaches must be established and communicated.

A.7.3 Termination and change of employment

A.7.3.1 Termination or change of employment responsibilities

The responsibilities with respect to information security that remain after change or termination of employment must be defined, communicated and enforced.

A.8 Asset management

A.8.1 Responsibility for assets

A.8.1.1 Inventory of assets

An inventory of the assets related to information or information processing must be maintained.

A.8.1.2 Ownership of assets

A person responsible for each of the previous assets must be appointed. This person must take care that the asset is properly managed throughout its entire lifecycle.

A.8.1.3 Acceptable use of assets

The use of information and information processing assets must be done according to a set of predefined rules.

A.8.1.4 Return of assets

Upon termination of employment, personnel must return all the assets of the organization in their possession.

A.8.2 Information classification

A.8.2.1 Classification of information

Information assets should be classified in different categories according to their sensitivity (to unauthorized disclosure or modification), according to the criticality for the organization, and according to legal requirements.

A.8.2.2 Labeling of information

Information assets must be labeled according to the previous classification.

A.8.2.3 Handling of assets

The organization must develop procedures for handling the assets in the different categories of the adopted classification scheme.

A.8.3 Media handling

Objective: To prevent unauthorized modification, removal or destruction of information stored in media.

A.8.3.1 Management of removable media

The organization must establish procedures to manage removable media in accordance to the adopted classification scheme.

A.8.3.2 Disposal of media

Media must be securely disposed when no longer needed. When choosing the disposal procedure must take into account the classification of the information contained.

A.8.3.3 Physical media transfer

During transportation, media must be protected to preserve the confidentiality and the integrity of the information.

A.9 Access control

A.9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities

A.9.1.1 Access control policy

The organization must establish an access control policy to the information and the information processing facilities.

A.9.1.2 Access to networks and network services

Access to the network and the network services

A.9.2 User access management

A.9.2.1 User registration and de-registration

A.9.2.2 User access provisioning

A formal process for providing and revoking access rights to users must be implemented.

A.9.2.3 Management of privileged access rights

The assignment of privileged access rights must be limited and controlled.

A.2.9.4 Management of secret authentication information of users.

The allocation of credentials to users must follow a formal process that guarantees that the security of the secret authentication information is preserved.

A.9.2.5 Review of user access rights

The access rights of users to information and information processing assets must be periodically reviewed by asset owners.

A.9.2.6 Removal or adjustment of access rights

The access rights of users to information and information processing assets must be removed or suspended upon termination or change of employment.

A.9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

A.9.3.1 Use of secret authentication information

Users must be required to follow the organization protocols for keeping the secrecy of authentication information.

A.9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

A.9.4.1 Information access restriction

Access to information and information processing systems must be limited according to the access control policy

A.9.4.2 Secure-log-on procedures

Access to information and information processing systems must be protected by a secure log-on procedure .A.9.4.3 Password management system Quality passwords must be required.

A.9.4.4 Use of privileged utility programs

The use of software that can overcome the limitations set by security controls must be restricted and their use controlled.

A.9.4.5 Access control to program source code

Access to the source code of an application must be controlled to prevent unauthorized modifications and to keep the intellectual property safe.

A.10. Cryptography

A.10.1 Cryptographic protocols

A.10.1.1 Policy on the use of cryptographic controls

The organization must define a policy for the use of cryptography.

A.10.1.2 Key management

Cryptographic keys must be kept securely throughout their entire lifespan.

A.11 Physical and environmental security

A.11.1 Secure areas

A.11.1.1 Physical security perimeter

The required level of security of each area must be defined according to the sensitiveness of the information that contains.

A.11.1.2 Physical entry controls

Physical barriers must be implemented to prevent unauthorized access to secure areas.

A.11.1.3 Securing offices, rooms and facilities

The organization must design the facilities taking physical security into account (e.g. by preventing confidential information and activities from being visible from the outside).

A.11.1.4 Protecting against external and environmental threats

The organization must take into account physical disasters (such as fire, flood, etc.) when designing physical security.

A.11.1.5 Working in secure areas

Working in secure areas must be tightly controlled.

A.11.1.6 Delivery and loading areas

Areas where unauthorized persons can enter should be controlled and isolated from other areas where information is processed.

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.1 Equipment siting and protection

Equipment must be protected to minimize the exposure to environmental threats and to unauthorized access.

A.11.2.2 Supporting utilities

Equipment should be protected from the failure of supporting utilities.

A.11.2.3 Cabling security

Cabling carrying power and telecommunications must be protected from any damage, interference, and interception.

A.11.2.4 Equipment maintenance

Equipment must be diligently maintained to prevent threats from happening.

A.11.2.5 Removal of assets

Information and equipment must not be taken outside the organization without a previous authorization.

A.11.2.6 Security of equipment and assets off-premises

The security of the assets that can be taken outside the premises of the organization must be designed taking into account the risks of working outside.

A.11.2.7 Secure disposal or re-use of equipment

Prior to disposal or re-use of an item of equipment, the organization must make sure that any confidential information present in the equipment and any software that gives access to confidential information have been securely removed.

A.11.2.8 Unattended user equipment

Users must be made aware of the risk of unattended equipment and make sure that they have the appropriate protection.

A.11.2.9 Clear desk and clear screen policy

The organization must establish a policy for clear desk and clear screen.

A.12 Operations security

A.12.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

A.12.1.1 Documented operating procedures

Information processing activities should be documented, and those documents made available to users that need them.

A.12.1.2 Change management

Changes to the organization, processes, systems and facilities must be planned and the information security risks assessed.

A.12.1.3 Capacity management

The organization must make sure that it has enough resources (human, facilities, and equipment) to make sure that the system performs as expected.

A.12.1.4 Separation of development, testing, and operational environments.

The separation between environments limits the risks of security breaches in the operational environment. For instance, by excluding developers from accessing personal data in the operational environment, and by allowing the detection of security issues in the development or the testing environment.

A.12.2 Protection from malware

A.12.2.1 Controls against malware

Effective protection against malware needs a combination of technical measures and personnel training.

A.12.3 Backup

A.12.3.1 Information backup

Backup copies of the information, the software, and the systems must be done and tested regularly.

A.12.4 Logging and monitoring

A.12.4.1 Event logging

User activities and system events must be logged, and the log reviewed to detect issues.

A.12.4.2 Protection of log information

Logs must be protected against unauthorized access and modification. In particular, against manipulation done by the system administrator.

A.12.4.3 Administrator and operator logs

The actions of the system administrator must be logged, and logs reviewed regularly.

A.12.4.4 Clock synchronization

To keep the consistency of logged events, the clocks of all systems must be synchronized.

A.12.5 Control of operational software

A.12.5.1 Installation of software on operational systems

The installation of software on operational environments must follow previously defined procedures that take into account all security-related aspects.

A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities

Information about newly discovered vulnerabilities should be obtained regularly, the exposure evaluated and actions to protect against them taken.

A.12.6.2 Restrictions on software installation

Uncontrolled software installation introduces many risks: lack of updates, vulnerabilities not being monitored, etc. The organization must establish a software installation policy.

A.12.7 Information systems audit considerations

A.12.7.1 Information systems audit controls

Audits of operational systems must be planned to minimize disruptions on the processes.

A.13 Communications security

A.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.1 Network controls

Networks should be controlled to protect the connected systems and information.

A.13.1.2 Security of network services

The security requirements of network services and the mechanisms to meet them must be identified and included in network-service agreements.

A.13.1.3 Segregation of networks

The separation of a network into different domains improves security.

A.13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 Information transfer policies and procedures

Transfers of information should be done according to relevant policies and procedures. Controls must be put in place to guarantee that information transfers are appropriate.

A.13.2.2 Agreements on information transfer

The transfer of information between the organization and external parties must be done securely and following an agreement between the involved parties.

A.13.2.3 Electronic messaging

Electronic messaging systems must be secured (confidentiality, integrity, and availability).

A.13.2.4 Confidentiality or non-disclosure agreements

The organization identify the need for non-disclosure agreements and reviewed in a regular manner.

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks.

A.14.1.1 Information security requirements analysis and specification

Information security must be included in the requirements of new and in the enhancement of existing processing systems.

A.14.1.2 Securing application services on public networks

Information sent over public networks must be secured against fraudulent activity; such as inspection and tampering.

A.14.1.3 Protecting application services transactions

Services must guarantee that any transaction is complete, authentic and secured against unauthorized disclosure.

A.14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.2.1 Secure development policy

The organization must establish a set of rules for the secure development of software within

A.14.2.2 System change control procedures

There must be a formal system for the control of changes; in particular, for major changes.

A.14.2.3 Technical review of applications after operating platform changes

A.14.2.4 Restrictions on changes to software packages

Vendor supplied software must have as least modifications as possible.

A.12.2.5 Secure systems engineering principles

A set of security principles that must guide any development must be established.

A.14.2.6 Secure development environment

A secure development environment must be established. This should consider the people, the processes and the technology used.

A.14.2.7 Outsourced development

Outsourced development activities must be supervised.

A.14.2.8 System security testing

Security aspects should be present in testing.

A.14.2.9 System acceptance testing

System security should be one of the aspects to consider in system acceptance.

A.14.3 Test data

Objective: To ensure the protection of data used for testing.

A.14.3.1 Protection of test data

Test data should be carefully selected. In particular, the use of personal identifiable data must be avoided.

A.15 Supplier relationships

A.15.1 Information security in supplier relationships

Objective: To ensure the protection of the organization's assets that are accessible by suppliers.

A.15.1.1 Information security policy for supplier relationships

A.15.1.2 addressing security within supplier agreements

A.15.1.3 Information and communication technology supply chain

Information security must be addressed in the agreements with suppliers.

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 Monitoring and review of supplier services

The delivery of services by suppliers must be regularly monitored.

A.15.2.2 Managing changes to supplier services

Changes to supplier services must be managed according to their criticality and risks.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 Responsibilities and procedures

Responsibilities and procedures are essential to respond promptly and effectively to security incidents.

A.16.1.2 Reporting information security incidents

Personnel must be aware of the need and the appropriate channel to report information security incidents.

A.16.1.3 Reporting information security weaknesses

All personnel using the information processing systems of the organization must be required to notify observed or suspected weaknesses.

A.16.1.4 Assessment of and decision on information security events

Information security events must be assessed and escalated to security incidents when needed.

A.16.1.5 Response to information security incidents

The response to information security incidents must follow documented procedures.

A.16.1.6 Learning from information security incidents

The knowledge that results from the analysis of security incidents must be used to reduce the risk of new incidents.

A.16.1.7 Collection of evidence

Procedures to collect as much evidence as possible must be established.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

A.17.1.1 Planning information security continuity

The organization must determine the information security requirements in case of a crisis or disaster. Unless otherwise specified, we must assume that information security requirements remain unaltered.

A.17.1.2 Implementing information security continuity

The processes, procedures, and controls to ensure that we keep the required level of information security during a crisis or disaster.

A.17.1.3 Verify, review and evaluate information security continuity

A.17.2 Redundancies

Objective: To ensure the availability of information processing facilities.

A.17.2.1 Availability of information processing facilities

There must be enough redundancy in the information processing facilities and equipment to meet the availability requirements.

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1 Identification of applicable legislation and contractual requirements

All regulatory and contractual requirements must be identified. The approach of the organization to meet such requirements must be documented.

A.18.1.2 Intellectual property rights

Appropriate procedures must be put in place to ensure compliance with intellectual property rights.

A.18.1.3 Protection of records

Some records need to be maintained to meet legal or regulatory requirements. Such records must be appropriately protected against loss, unauthorized access, and unauthorized modification.

A.18.1.4 Privacy and protection of personally identifiable information

Personal data protection requirements in relevant legislation must be met.

A.18.1.5 Regulation of cryptographic controls

The use of cryptographic controls may be subject to external regulations. Relevant regulations must be met.

A.18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with organizational policies and procedures.

A.18.2.1 Independent review of information security

Independent reviews of the approach to information security at regular intervals is necessary to ensure its effectivity.

A.18.2.2 Compliance with security policies and standards

The compliance of information processing systems with security policies and standards must be regularly reviewed.

A.18.2.3 Technical compliance review

Technical compliance with security policies and standards must be review regularly.

6.6 Residual risk computation

Once we have established the security controls to apply, we need to recompute the risk. This is the residual risk. In general, security controls are classified according to the objective they have: preventive, detective, corrective, dissuasive, recovery and compensatory. These controls may have two effects on the risk: reduce the impact and the probability of an incident.

In the previous section, we gave some guidelines to select the controls to apply. These guidelines are merely indicative and do not have a predefined effect on the risk. It is the controller who has to choose controls to apply and describe and justify the effects that these controls have on the impact and the probability.

Residual risk is calculated based on residual impact and residual probability, using the table in section 4.6. If the residual risk is high, it is necessary to propose new controls to reduce it. If it is not possible to reduce it, we need to consult the competent data protection authority about the suitability of the data processing before it starts.