agencia
española
protección
datos

Risk Management and Impact Assessment in the Processing of Personal Data

June 2021

EXECUTIVE SUMMARY

This document is a guide to the management of risks to the rights and freedoms of data subjects applicable to any processing operation, regardless of the level of risk. In addition, and for cases of high-risk processing, it incorporates the necessary guidelines for carrying out the Data Protection Impact Assessment (DPIA) and, where appropriate, the prior consultation referred to in Article 36 of the GDPR.

This guide updates and unifies those presented more than three years ago by AEPD: the “Practical Guide for Risk Analysis for the Processing of Personal Data" and the "Practical Guide for Impact Assessments on Personal Data Protection". The aim of the guide is to incorporate lessons learned in the application of risk management in the field of data protection, and new criteria and interpretations, both from the AEPD and from the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS). In addition to drawing on accumulated experience, it aims to improve materials aimed at assisting compliance by controllers, providing a unified view of risk management and the DPIA. Finally, this document will facilitate the necessary integration of risk management for rights and freedoms, and in general compliance with the GDPR, in the management and governance processes of the entities.

The guide consists of three main sections divided into chapters: a first section with a description of the fundamentals of risk management for rights and freedoms, a second section that includes a basic methodological development for the application of risk management for rights and freedoms, and a final section, focused on cases in which a Data Protection Impact Assessment must be carried out, with specific methodological guidelines in this respect.

This document is preferably addressed to Controllers, Processors and Data Protection Officers (DPOs).

Keywords: data protection, proactive responsibility, risk, impact assessment, DPIA, management, governance, policies, impact, measures, safeguards, data protection by design, data protection by default, prior consultation, DPO, rights, security.

TABLE OF CONTENTS

TABLE OF CONTENTS OF FIGURES

TABLE OF CONTENTS OF TABLES

I. INTRODUCTION

In any new activity, prior reflection in order to identify potential problems and anticipate future difficulties allows rational decisions to be made and to act with guarantees of success. The effort put into evaluating the possible consequences[1] of future actions must be proportionate to the potential harm or impact that could result therefrom. When this approach is applied to the governance of an organisation, it is referred to as "risk management". The degree of effectiveness and efficiency of such management determines the entity's level of maturity.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation, hereinafter 'GDPR') aims to align the protection of personal data with the evolution of increasingly complex processing activities[2,3]. This entails implementing a compliance model called accountability. This model is processing-oriented and its management is based on a risk-based approach. Therefore, the GDPR is a model that is compatible with, and can be integrated into, the modern management of any organisation.

Prior to the full implementation of the GDPR, three years ago, the AEPD presented the guides entitled "Practical Guide for Risk Analysis for the Processing of Personal Data" and "Practical Guide for Impact Assessments on Personal Data Protection". Since then, and within the framework of the lessons learned from the implementation of risk management, new criteria and interpretations have been developed, both by the AEPD and by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS). This guide unifies the two previous guides for several purposes: to gather accumulated experience, to improve materials to assist compliance by controllers, to provide a unified view of risk management and the DPIA, and to facilitate the integration of risk management into the management and governance processes of organisations.

This document is a guide to the management of risks to the rights and freedoms of data subjects applicable to any processing operation, regardless of the level of risk. In addition, and for cases of high-risk processing, it incorporates the necessary guidelines for carrying out the Data Protection Impact Assessment (DPIA).

The guide is divided into three main sections:

- A first section containing the fundamentals of risk management for rights and freedoms, which is organised in the following chapters.
    - Concepts associated with risk management

[1] Short- and long-term consequences.

[2] Recital 6: *"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."*

[3] Recital 7: *"Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced."*

    - Management process of the risks posed to rights and freedoms
    - Risk governance
- A section with the basic methodological development for the practical application of risk management for rights and freedoms, organised in the following chapters:
    - The description and contextualisation of the processing
    - Identifying and analysing sources of risk to rights and freedoms
    - Assessing the level of risk related to the processing
    - Controls to reduce risk
    - Residual risk assessment and review
- For when a Data Protection Impact Assessment (DPIA) is required, a section dedicated to methodological guidance with chapters:
    - The data protection impact assessment.
    - Analysis of the obligation to carry out the DPIA
    - Analysis of the need to complete a DPIA
    - Assessment of the necessity and proportionality of the processing
    - Documentation obligation
    - Seek the views of data subjects.
    - Prior consultation of the Supervisory Authority

This document is aimed, preferably, at data controllers, data processors and data protection officers (DPOs). As set out in Article 24 of the GDPR, the controller is responsible for ensuring that measures are taken to manage the risk to the rights and freedoms of data subjects. In the case of high-risk processing, the GDPR establishes that it is the controller's obligation to carry out the DPIA with the advice, where appropriate, of the DPO (Articles 35 and 39 GDPR).

On the other hand, Article 28(3)(c), (f) and (h) establishes the obligation of the processor to assist the controller and to make available to the controller the tools and information to demonstrate compliance. Accordingly, this document is also aimed at data processors in the context of the development of these obligations.

Finally, in order to be able to comply with the functions set out in Article 39 of the GDPR, this guide is almost mandatory reading for Data Protection Officers.

In closing this introduction, and beyond the obligation to comply with the principle of proactive responsibility in the GDPR, it is important to underline a key issue: avoiding risk identification and management activities in a processing operation, ignoring them, or procrastinating the duties and obligations of the controller, is a major source of future problems for data subjects, citizens, users, employees and the controller itself. The greatest harm will not arise from high-risk processing when they are well managed. Negative impacts, in the medium and long term, will occur in poorly managed processing, where threats and the severity of their consequences are ignored.

SECTION 1: FUNDAMENTALS OF THE MANAGEMENT OF THE RISKS TO THE RIGHTS AND FREEDOMS

II. CONCEPTS ASSOCIATED WITH RISK MANAGEMENT

Risk management is a key element in the processes of any organisation and is an inherent part of the management of any entity, project or human activity.

Risk management consists of a set of ordered and systematised actions with the purpose of controlling the possible (likelihood) consequences (impacts) that an activity may have on a set of goods or elements (assets) to be protected. Risk management requires an analysis, i.e. a critical and objective reflection of a processing, requires decisions to be taken and translated into concrete actions (controls) that minimise the impact on assets to tolerable levels.

The GDPR requires objective[5] identification, assessment and mitigation[4] of the risk to the rights and freedoms of individuals in the processing of personal data. Mitigation has to be done by adopting technical and organisational measures that ensure and, moreover, demonstrate the protection of these rights[6]. These should be determined by reference to the nature, scope, context and purposes of the processing[7]. Likewise, those measures shall be reviewed and updated where necessary[8]. Ultimately, the GDPR requires a risk management process[9] for the rights and freedoms of data subjects.

In compliance with the principle of accountability, risk management must be documented. However, it is important to differentiate between reports documenting risk management actions and risk management itself. Risk management is not a document but a process that is translated into facts and documented.

A. RISK MANAGEMENT

Risk management is one of the pillars of the management of any organisation. When an entity intends to launch a new product or service with guarantees, it must manage the elements of uncertainty that arise from its nature, scope, context and purpose. The ISO standards[10] define this activity as the "risk based thinking" (RBT). The RBT is, with the process orientation(processing), one of the two pillars for quality management in any entity or, in other words, it is the "language" spoken by modern management systems in organisations.

[4] Recital 77 "...the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk..."

[5] Recital 76 "...Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk..

[6] Article 24 "Taking into account ... the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate ..."

[7] Recital 76 "The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing."

[8] Article 24 Those measures shall be reviewed and updated where necessary".

[9] Footnote 6 of the WP248 Guidelines interprets: It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analysed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly.

[10] ISO 9000 family of standards

This approach is thus established in quality standards, such as the ISO 9001 family, forms part of the syllabus of business schools, is found in the methodologies of analysis and risk management of information systems in Public Administrations[11] and is even included in the Criminal Code itself[12]. Risk management is a guarantee for the sustainable growth of any entity[13].

The ISO standards[14] standards define the concept of "risk" as the *"effect of uncertainty on the achievement of objectives"*, meaning any positive or negative deviation from what was initially planned, taking into account that objectives can be of different types depending on the scope of activity of an organisation.

When an organisation has to develop a new activity, which will take the form of a processing, elements of uncertainty arise. Uncertainties manifest themselves from different perspectives. For example, an entity must be able to ensure that it has the necessary capital to carry out the new initiative, i.e., it must manage the financial risk. In order to start up a project, it is not only necessary to have the capital, but also to have the necessary resources (human and material), in time, place and form, which are subject to problems of availability, suitability, etc., which implies managing the risk of implementing the project itself. The implementation of this will use novel techniques and technologies that generate uncertainties in their performance, which implies a risk management of technical reliability.

Other risks that need to be managed are: security risk to people; security risk in relation to business continuity; fraud risks; determining whether the activity will generate sufficient benefits, tangible or intangible, to compensate for the investment, i.e. performing cost/benefit analysis, etc.

Moreover, the new activity is not isolated from the rest of the entity. The processing takes place in the internal context of the organisation, so the impact on other organisational activities (e.g., on the use of personnel, space, etc.) must be analysed, as well as the opportunity cost risk of relegating other possible initiatives due to limited resources.

Furthermore, the activity and the organisation operate in a changing social and economic context that needs to be interacted with. For example, the business has to comply with regulations (compliance risk) and will have to adapt to future regulatory changes (legal risk).

[11] MAGERIT https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[12] Article 31a on the criminal liability of legal persons. Paragraph 2 on exemption from liability: "1. the management body has adopted and effectively implemented, prior to the commission of the offence, organisational and management models that include the appropriate supervision and control measures to prevent offences of the same nature or to significantly reduce the risk of their commission"

[13] “Risk in review: decoding uncertainty, delivering value” PWC https://www.pwc.com/gx/en/audit-services/publications/assets/pwc- risk-in-review-2015.pdf

[14] ISO 31000:2018(EN) Risk management and ISO 31010:2019 Risk management. Risk assessment techniques

Risks of civil[15] or criminal liability that may arise from direct or collateral effects of the processing must be managed. In addition to the effects of the environment on the organisation, it is necessary to analyse the effects of processing on the environment through environmental risk analysis or social impact analysis (social responsibility), etc.

Examples of different perspectives on risk management	
The processing itself	Financial risk
	Project risk
	Fraud risk
	Safety risks to persons (occupational)
	Cost/benefit
	Technical reliability risk
	Business continuity risks in I.S., etc.
Processing in the internal context of the organisation	Impact on other processing in the same organisation, directly or indirectly
	Opportunity cost, etc.
Processing in the external regulatory, social and economic context	Legal and compliance risk
	Risks of civil or criminal liability
	Environmental risk
	Social impact
	Risk to rights and freedoms, etc.

Table 1 Examples of different perspectives on risk management

Risk management should therefore be understood as a general methodology that integrates different management objectives (financial, legal, labour, social, etc.)[16.]

[15] Risk that in the event of the occurrence of the incident associated with it causes an increase in the obligations of those who have been civilly liable for the damage or harm caused to third parties.

[16] Virtually everyone is managing risks from different perspectives and in an integrated way. For example, when purchasing a vehicle, they have analysed the ability and means of payment (financial risk), they have analysed the risk of purchasing the vehicle from third parties rather than from the dealer (fraud risk), the mechanical reliability of one brand versus another (technical risk), which brand performs better in the event of an accident (safety risk), whether it is worth the investment in relation to its intended use (cost/benefit analysis), whether it is environmentally friendly (environmental risk), the legal and economic protection against possible damage to third parties (liability risk), whether it would be better to buy a house rather than a car (opportunity cost analysis), the possibility of types of vehicles being made illegal in the future (legal risk), etc. Any judicious person will carry out this analysis, balancing pros and cons, in a comprehensive way and taking decisions and measures to minimise risk. The difference between one person and another in making this analysis will be found in the depth of the analysis, and in the formality used for its study. Both will depend on the impact this, or any other, activity can have on their lives.

B. RISK MANAGEMENT IN THE GDPR

The GDPR refers to the term "risk" seventy-three times throughout the text, specifically in Articles 4.24, 23.2.g, 24.1, 25.1, 27.2.a, 30.5, 32, 33, 34, 35, 36, 39.2, 49.1, among others. In particular, Article 24(1) states:

> *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

The 'risk-based approach' is developed in the 'Statement on the role of a risk-based approach in data protection legal frameworks WP218' of the Article 29 Working Party17 (hereinafter the WP218 Statement) and is not a novel concept in the data protection framework18.

The GDPR establishes the obligation to manage the risk to the rights and freedoms of individuals posed by a processing operation. This risk arises both from the very existence of the processing itself and from the technical and organisational dimensions of the processing. The risk arises from both automated data processing and manual data processing, the human elements and the resources involved. The risk arises from the purposes of the processing and its nature, as well as from its scope and the context in which it takes place.

The GDPR does not establish a practical-methodological approach to risk management. In that respect, the GDPR leaves freedom for this risk management for rights and freedoms to be integrated with the rest of the organisation's risk management resources, policies and governance.

In general, the GDPR also does not require any explicit formality requirements for the execution of risk management, without prejudice to the accountability obligations mentioned above. However, for high-risk processing, the GDPR does establish minimum requirements for its management. These derive, in particular, from the obligations set out in Articles 35 'Data Protection Impact Assessment' (DPIA), and Article 36 of the GDPR. In this regard, the European Data Protection Board has developed the document "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679"19 (throughout this text referred to as WP248 Guidelines).

The WP248 Guidelines define the concepts of "risk" and "risk management":

> *A “risk” is a scenario describing an event and its consequences, estimated in terms of severity and likelihood*

[17] Statement on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[18] WP218 Statement “The so-called “risk-based approach” is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20). The legal regime applicable to the processing of special categories of data (Article 8) can also be considered as the application of a risk-based approach...”

[19] https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.

The WP248 Guidelines include recommendations for both the conduct of DPIA and risk management in general.

C. RISKS TO THE RIGHTS AND FREEDOMS

The risk to rights and freedoms mainly concerns, as the WP248 Guidelines state, the rights to data protection and privacy[20].

Recital 75[21] develops the concept of risk to rights and freedoms as any unintended effect or consequence on data subjects or not foreseen in the processing of personal data itself, capable of causing damage or prejudice to their rights and freedoms, specifying, inter alia: physical, material or immaterial damage, problems of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorised reversal of pseudonymisation, economic or social damage, depriving data subjects of their rights and freedoms, preventing them from exercising control over their personal data, etc.

More specifically, the WP248[22] Guidelines themselves interpret the protection to extend to other fundamental rights. Freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion are explicitly mentioned.

Furthermore, WP218 Statement interprets that, in the risk-based approach, the protection of these rights has to be carried out by assessing both the impact on the person concerned of the processing in question and the overall social impact it may have. In the latter case, a concrete example is given, such as the loss of social trust[23]. Therefore, it is not only necessary to manage the risks to the person whose data are being processed, but those of all individuals or groups of individuals affected24 by the processing.

[20] WP248 Guidelines: "As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy".

[21] The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing **which could lead to physical, material or non-material damage**, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

[22] ...but may also involve other fundamental rights such as freedom of speech, freedom of thought,
freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

[23] 11/ The risk-based approach …, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)

In conclusion, the focus of risk management in the GDPR is the protection of the individual, in his or her individual and social dimension, as the data subject or person affected by the processing. Although it has a collateral relationship, risk management for rights and freedoms is not aimed at protecting the controller's or processor's own interests in relation to, for example, the continuity of processing, its effectiveness or efficiency, regulatory compliance or in relation to the possible business activities of the processor and controller.

D. MANAGEMENT OF COMPLIANCE RISK VS. THE RISKS POSED TO RIGHTS AND FREEDOMS

Compliance risk can be defined as the management of an entity's risk of incurring legal or administrative sanctions, significant financial or reputational losses due to non-compliance with legal regulations, internal rules and codes of conduct applicable to the activities, in this case, of a controller or processor.

Risk management for rights and freedoms is not aimed at managing the risk to the organisation arising from non-compliance with regulations. The former is data subject-oriented, as noted in the previous section, while the latter is risk management that focuses on protecting the interests of the institution. Therefore, non-compliance or potential non-compliance with the principles and rights set out in the GDPR and the developing regulations is not the subject of a risk management of the risk to the rights and freedoms that a processing operation may cause to data subjects.

WP218 Statement[25], interprets that the fundamental rights and principles set out in the GDPR with which controllers must comply must be guaranteed, regardless of the characteristics of the processing and the process of managing the risk to rights and freedoms.

[24] Often the aim of a processing operation is none other than to classify people into a specific group, although the usual dimension is the individual, often decisions taken by a controller may affect the rights of groups of people: https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo

[25] 2/ Rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved (e.g. right of access, rectification, erasure, objection, transparency, right to be forgotten, right to data portability).

4/ Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects.

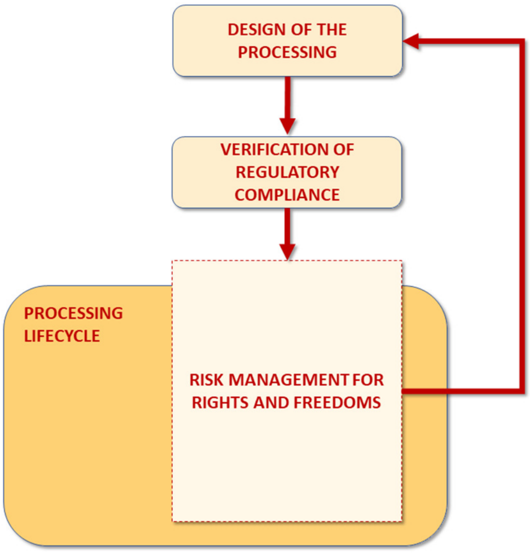

DESIGN OF THE PROCESSING
VERIFICATION OF REGULATORY COMPLIANCE
PROCESSING LIFECYCLE
RISK MANAGEMENT FOR RIGHTS AND FREEDOMS

Figure 1 Compliance as a Prerequisite for Risk Management

It is a misinterpretation to understand the risk approach of the GDPR as a way to replace compliance requirements with technical and organisational controls or measures. Even less so, the GDPR's risk approach is not geared towards addressing the possible consequences for data subjects of a possible breach of the law. In particular, legal, technical and organisational measures that might arise as a result of risk management for rights and freedoms do not justify, for example, the absence or misuse of a certain legal basis for a processing operation, nor, for example, the absence of any of the exceptions lifting the prohibition on processing special categories of data. That is to say, the legal basis cannot be substituted or supported by the concurrence of alternatives to compliance itself, including, where appropriate, the necessary assessment of legitimate interest[26].

In short, it would not be lawful to replace any of the principles of the GDPR with technical and organisational measures aimed at replacing those principles or at mitigating the possible consequences that such non-compliance could have on the data subjects concerned.

In the same vein, the management of risk to rights and freedoms cannot be solved by the use of legal safeguards based on a diversion of liability to third parties. The obligation to guarantee the rights and freedoms rests with the controller, as WP248 Guidelines note 10 makes clear:

> *... Controllers cannot escape their responsibility by covering risks under insurance policies.*

Thus, an insurance policy that covers the damages that may be generated for the organisation, or a contractual agreement that seeks to displace the responsibilities to a third party it is not a measure to manage the risk to rights and freedoms.

[26] WP218 Statement: 12/ The legitimate interest pursued by the controller or a third party is not relevant to the assessment of the risks for the data subjects. It is in applying the balancing test under the criteria for making the data processing legitimate under the Directive (Article 7 f.) or of the draft regulation (Article 6 f.) that the legitimate interest should be taken into account.

The cost/benefit balance, in economic or financial terms, derived from the lack of compliance with data protection regulations should not be interpreted, in any case, as risk management for the rights and freedoms of natural persons, but could even be considered by the Supervisory Authority as a possible benefit obtained from the infringement itself[27] and a possible aggravating factor[28].

Legal Guarantee	Management of the risks posed to rights and freedoms.
Contract with the processor complying with the requirements of Article 28 of the GDPR	It is a regulatory compliance obligation, not risk management
Insurance policy to cover the organisational responsibility for a possible breach of the GDPR	It involves risk management of compliance, but not with regard to rights and freedoms.
The signing of a confidentiality agreement by personnel processing certain data.	It can be a risk management measure for rights and freedoms, insofar as it does not relax the obligations of the responsible party, but seeks to ensure the commitment of the personnel processing the data.

Table 2 Examples of Legal Safeguards and their relation to Risk Management

Risk management for rights and freedoms aims at assessing the impact and likelihood of harm to individuals, at the individual or societal level, as a result of the processing of personal data. In contrast, compliance risk management aims to provide the controller with a tool to verify the degree of compliance with the legally required obligations and precepts in relation to a processing activity. Therefore, prior to the risk management process and as a *sine qua non* condition for undertaking a processing activity, it is necessary to systematise the verification of regulatory compliance throughout the entire processing lifecycle.

The AEPD makes available to controllers and processors a document that contains a Compliance Checklist and a Roadmap to ensure Compliance with data protection regulations which may be useful when analysing the degree of compliance with data protection regulations.

[27] Recital 149: “Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation.”

[28] Article 83.2.k: Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

E. RISK MANAGEMENT IN ALL PROCESSING

All personal data processing activities entail a risk for the individuals whose data are processed and, in particular, for their rights and freedoms. Even in those cases in which the data controller, either because of the type of data or because of the type of activity of the organisation, could assume the existence of a low risk for data subjects or even the absence of risk.

The WP248 Guidelines clarify the importance of performing risk management on processing even when processing are not high risk:

> *...The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects.*

In the same vein, in relation to the general obligations of the data controller and data processor, Article 28 of Organic Act 3/2018, of 5 December, on Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD, as per the Spanish acronym) sets out the need to take into account the risks that could arise as a result of the processing of personal data.

Therefore, the concept of 'zero risk' does not exist when we talk about risk management, in particular when we talk about the risks that personal data processing may pose. There will always be an inherent or initial risk involved in any processing and, once measures and safeguards have been put in place to minimise it, there will still be a residual risk.

WP218 Statement interprets the risk approach as a scalable process that can be adapted to the specific processing situation. The risk-based approach must be proportionate, and the implementation of the risk management process for rights and freedoms must be guided by principles of effectiveness and efficiency. The complexity of the risk management process has to be adjusted not to the size of the entity, the availability of resources, the speciality or sector of the entity, but to the potential impact of the processing activity on data subjects and the difficulty of the processing itself. If an entity intends to undertake a processing and does not have the capacity to do the necessary risk management, it will be obliged to seek some form of assistance, such as external consultancy, to do so in an appropriate manner.

When processing operations are low risk, the AEPD has tools to guide and facilitate their management. The AEPD also provides tools to help carry out a first analysis in high-risk processing.

F. PROACTIVE MANAGEMENT IN RISK MANAGEMENT

WP218 Statement[29] interprets that the risk-based approach must go beyond an approach limited to reacting to harm to the data subject. Risk management should not be reduced to merely managing the consequences for the data subject, as in the case of a personal data breach. Risk management must include the preventive approach.

[29] 11/ The risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage and should take into consideration every potential as well as actual adverse effect.

Furthermore, when determining the risk factors to manage, the present context and potential future contexts must be taken into account. Risk management requires a long-term assessment, especially in scenarios where the impact could result in a very high level of harm to data subjects or society.

G. RISK MANAGEMENT AS A PROCESS

Risk management involves activities such as contextualising, identifying, analysing, evaluating, acting and reviewing. Risk management must be approached as a cross-cutting process throughout the organisation and connected with the rest of the existing processes in order to achieve a global, comprehensive, effective and efficient risk management framework that encompasses the organisation as a whole and in all its dimensions. The commitment of the organisation's controllers to such management is a key factor for success.

WP218 Statement interprets that risk management for rights and freedoms should not be reduced to a "*checkbox exercise*"[30]. On the contrary, risk management, as understood by the ISO 31000[31] standard, is a process consisting of a set of activities and tasks to control the uncertainty related to a threat, through a sequence of initiatives or actions.

Risk management applications, guides or checklists can be valuable support tools, providing useful information for risk management. However, it should be borne in mind that the final analysis, decision-making and implementation of the action plan are the sole responsibility of the management and potential implementers of such measures, with the tools being merely instruments to assist and support management tasks.

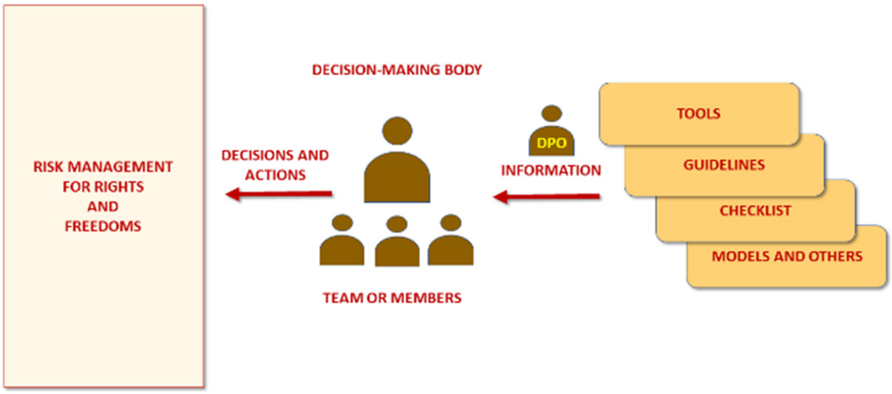


Figure 2 Decision Support and Decision-Making

The risk management process should have at least the following stages:

[30] Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is sufficiently protected.

[31] 4.4.2 Implementation of the risk management process. Risk management should be implemented in a way that ensures that the risk management process described in Chapter 5 is implemented through a risk management plan at all relevant levels and functions of the organisation as part of its practices and processes.

- Description of the processing, both as regards its nature, scope, context and purposes.
- Identification and analysis of risks in processing.
- Assessment of the level of risk and determination of whether a DPIA is appropriate or necessary.
- Risk Management.
- Monitoring and verification of the effectiveness of the measures taken and decision on when a process of review and reassessment of the measures is necessary.

There are two prior tasks: the determination of the design of the processing, at the highest level, and the prior analysis of the requirements for compliance with the provisions of data protection regulations:

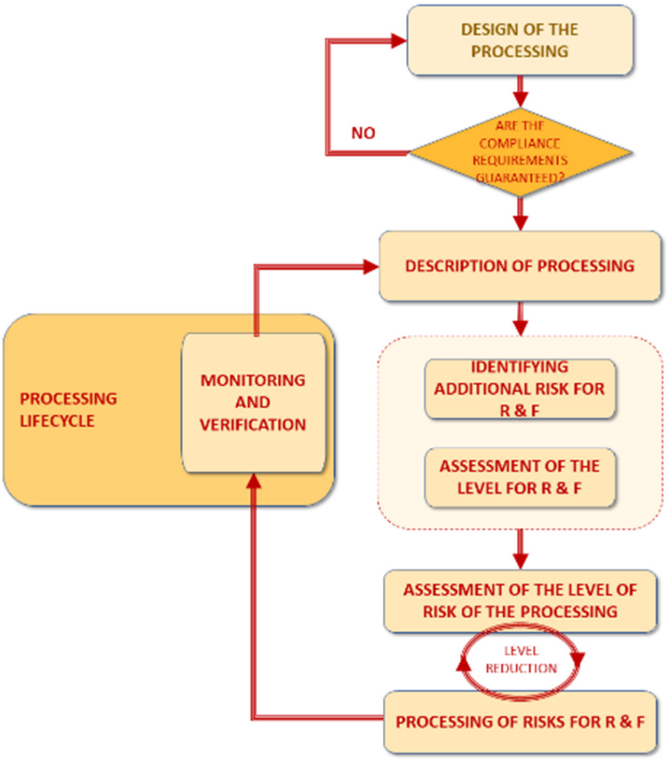

DESIGN OF THE PROCESSING
NO
ARE THE COMPLIANCE REQUIREMENTS GUARANTEED?
DESCRIPTION OF PROCESSING
PROCESSING LIFECYCLE
MONITORING AND VERIFICATION
IDENTIFYING ADDITIONAL RISK FOR R & F
ASSESSMENT OF THE LEVEL FOR R & F
ASSESSMENT OF THE LEVEL OF RISK OF THE PROCESSING
LEVEL REDUCTION
PROCESSING OF RISKS FOR R & F

Figure 3 Basic Outline of the Risk Management Process

These steps must be implemented in a way that makes it possible to establish to what extent a processing activity, due to the context, its characteristics, the type of data processed, its extent, its purposes, or the characteristics of the data subjects, is likely to have consequences (impact) on the rights and freedoms of natural persons. In addition, a continuous monitoring sub-process should be included, which should be understood as the management of the continuous improvement of the risk analysis and management process.

As it is a process, it must be captured and documented in the organisation's policies[32].

H. INTEGRATION IN THE MANAGEMENT OF THE ORGANISATION

ISO 31000[33] states that risk management must be integrated with the rest of the entity's processes, in particular in policy, planning and review of the processing, in order to be relevant, effective and efficient.

In other words, risk management cannot be done in isolation, independently or after the design and/or implementation of a processing. Risk management for rights and freedoms needs to be integrated into the governance and policies of the entity[34] in order to be effective and efficient and not merely a formal formality.

In this sense, and referring to the DPIA, the WP248 Guidelines state, in relation to risk management, that risk management:

> *...is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;*

Among the processes with which it must be integrated are all those relating to risk management from other perspectives: financial, fraud, opportunity cost, continuity of processes, image, impersonation, business, environmental, personal safety, etc., which must be understood in a comprehensive manner.

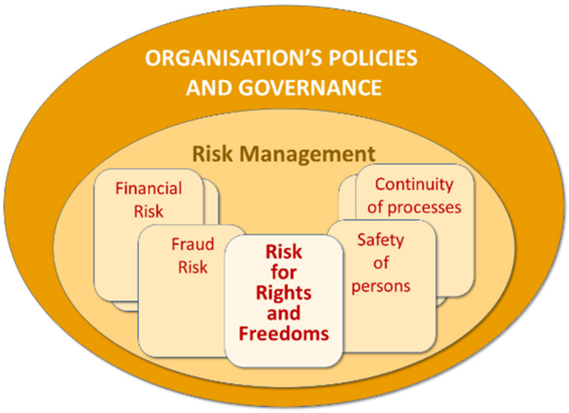


Figure 4: Integration of Risk Management for Rights and Freedoms in the rest of the Risk Management Processes of the Organisation.

[32] Article 24 of the GDPR: Responsibility of the controller:

> 2- Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

[33] Risk management should be integrated into all organisational practices and processes in a way that is relevant, effective and efficient. The risk management process should be part of the organisation's processes, not independent thereof. In particular, risk management should be integrated into policy development, business and strategy planning and review, and change management processes.

[34] In fact, the integration of all GDPR compliance actions would be desirable.

Within an organisation, all these analyses should not be managed independently, as this would make them ineffective; they should rather be analysed in a unified way in order to reach a single conclusion. In this way, the controller can reach a decision in the framework of a holistic approach that takes into consideration the overall processing context, its requirements and constraints, within a common risk management framework for all processes in the organisation.

A particular case of this integrated management is represented by the obligations of the controller with regard to the notification of personal data breaches to the Supervisory Authority, as well as the communication of these to the data subjects themselves. In this case, the assessment of the risk to the rights and freedoms of data subjects that the data breach may represent should in no case be lower than the assessment that would have been made in the framework of the risk analysis of the processing. As mentioned above, risk management and breach management are two tasks that must be managed together to avoid inconsistencies that could have a negative impact on the process of managing the processing of personal data or on the data subjects themselves.

ASSESSMENT OF
RISKS OF THE PROCESSING
ASSESSMENT OF RISKS OF
A PERSONAL DATA BREACH

Figure 5Risk Assessment of the Processing and of a Data Breach

I. ROLE OF PROCESSORS, DEVELOPERS AND SUPPLIERS

The management of the risk to the rights and freedoms is an obligation of the data controller, as set out in Article 24(1) of the GDPR:

> *Taking into account ... as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.*

In the case of commissioned processing, the GDPR establishes the obligation to assist the controller in carrying out risk management, taking into account the nature of the processing and the information at its disposal, in Article 28, paragraphs 3.c[35], f[36] and h[37], as well as in Recital 83[38]. In order to effectively carry out these duties, the processor must carry out risk management for rights and freedoms at least within the limits of the subject matter of the assignment.

On the other hand, a developer or provider of a product or service with which several controllers will carry out different data processing operations may carry out risk management for rights and freedoms. In that case the risks should be incorporated into

[35] c) takes all measures required pursuant to Article 32.

[36] f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor.

[37] h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

[38] In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.

the risk management process of the processing intended to be carried out by the controller. This process should be covered by the contractual guarantees corresponding to the purchase of the product or service.

In any case, regardless of the management carried out by processors, developers or suppliers, the controller will continue to maintain the obligation to carry out its own risk management, or a DPIA when the processing operations it carries out are likely to entail a high risk to the rights and freedoms of data subjects.

J. MANAGEMENT OF THE RISKS TO THE RIGHTS AND FREEDOMS AND DPIA

The GDPR sets out the obligations relating to the data protection impact assessment (DPIA) mainly in Articles 35 and 36. As stated in Article 35:

> *"Where a type of processing ... is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out*
>
> *... an assessment of the impact".*

The GDPR does not require that any processing of personal data must be subject to a DPIA, but it does require it to be carried out when there is a likelihood of a high risk. The existence of a reasonable degree of presumption that the processing may involve a high risk makes it imperative that a DPIA be conducted.

1. Definition of DPIA as a Process that compels Action

The text of the Regulation does not contain a definition for the term 'data protection impact assessment' or DPIA. The EDPB does develop the definition of DPIA in the WP248 Guidelines as:

> *"... process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them"*

Accordingly, the EDPB considers that the DPIA is a "*process*" and, therefore**:**

- Reducing DPIA to a one-off, isolated activity in time is incompatible with the concept of process as interpreted by the WP248 Guidelines.
- The DPIA needs to be documented[39],but the DPIA is more than the report reflecting its output.
- The DPIA must assess risks by "*identifying measures to address them*". The DPIA obliges the controller to act and has a greater dimension than a mere formalism embodied in a document to which minimal changes can be made to adapt it to any processing.

The DPIA is a process of analysis of a processing operation that extends over time, throughout the entire lifecycle of a personal data processing operation, and that must be reviewed on an ongoing basis, "at least when there is a change of the risk represented by processing operations" (art. 35.11 of the GDPR)

[39] In order to support the data controller in carrying out this process, the AEPD has published models for documenting the result of this process before the Supervisory Authority. These templates make it easier for the controller to properly document a prior consultation.

2. Integrating DPIA and Risk Management

The DPIA is part of the process of managing risks to the rights and freedoms of individuals with regard to the processing of their personal data. In the definition of the EDPB, one of the missions of the DPIA is "to help manage the risks to the rights and freedoms of natural persons arising from processing".

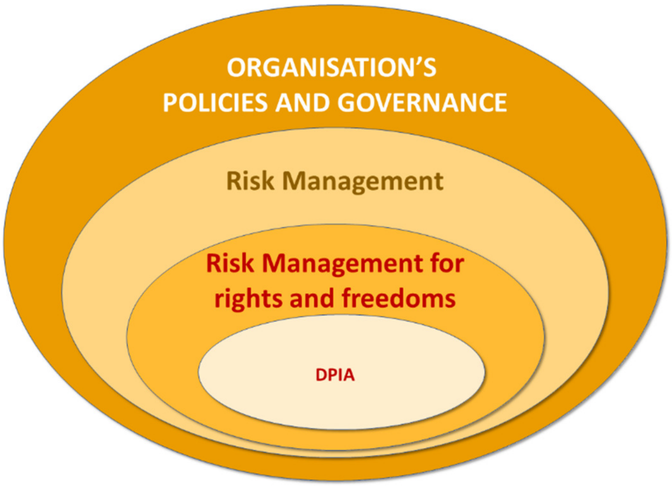


Figure 6: Integration of the DPIA for Risk Management Requirements for Rights and Freedoms

DPIA and risk management are integrated activities. Once the decision is taken to carry out a DPIA, it forms an indivisible part of the management of risks to rights and freedoms. Thus, it is not possible to implement a DPIA if there is no risk management for rights and freedoms and it is not carried out within the framework of the DPIA.

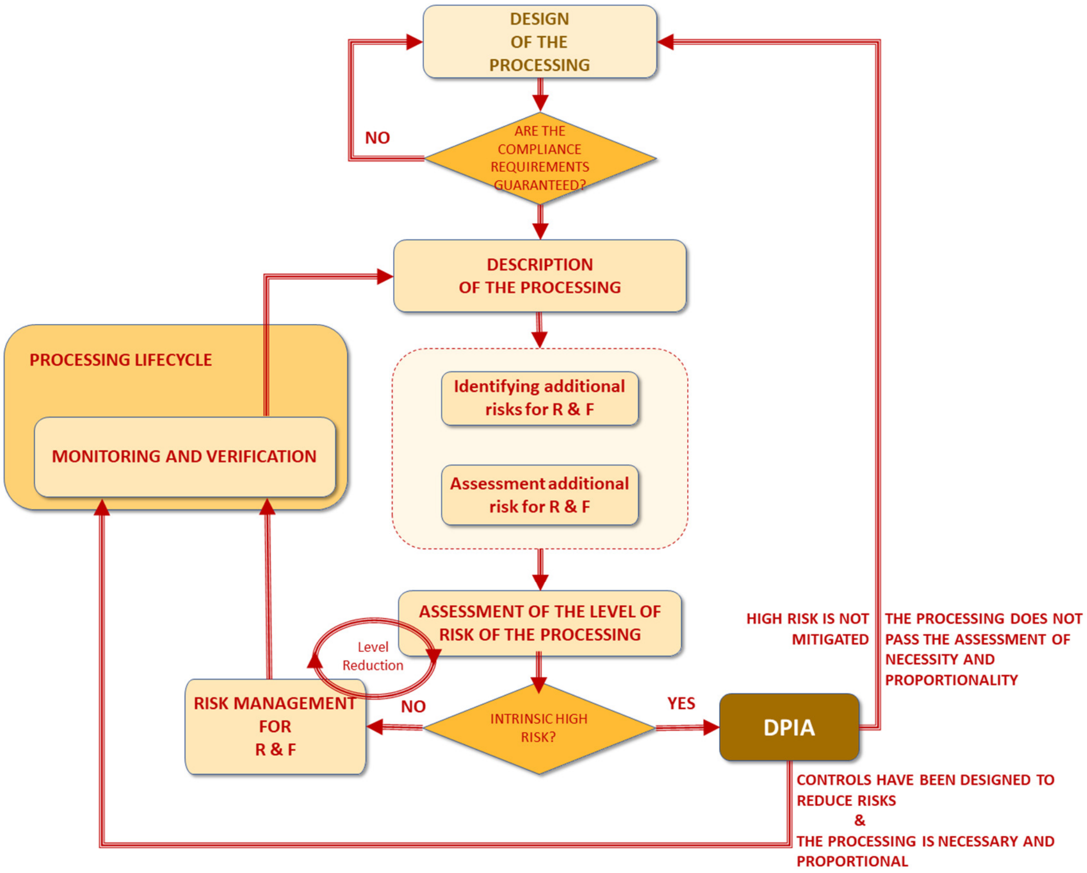

DESIGN OF THE PROCESSING
NO
ARE THE COMPLIANCE REQUIREMENTS GUARANTEED?
DESCRIPTION OF THE PROCESSING
PROCESSING LIFECYCLE
MONITORING AND VERIFICATION
Identifying additional risks for R & F
Assessment additional risk for R & F
ASSESSMENT OF THE LEVEL OF RISK OF THE PROCESSING
Level Reduction
RISK MANAGEMENT FOR R & F
NO
INTRINSIC HIGH RISK?
YES
DPIA
HIGH RISK IS NOT MITIGATED
THE PROCESSING DOES NOT PASS THE ASSESSMENT OF NECESSITY AND PROPORTIONALITY
CONTROLS HAVE BEEN DESIGNED TO REDUCE RISKS & THE PROCESSING IS NECESSARY AND PROPORTIONAL

Figure 7: Basic Outline of the Risk Management Process including the DPIA

3. The DPIA Expands Risk Management Requirements

Within the framework of the DPIA, the GDPR adds additional requirements to the risk management of rights and freedoms, adding a higher degree of detail, in particular in the depth of the analysis, in the *accountability* requirements (e.g. documentation and involvement of the DPO) and in the control by Supervisory Authorities.

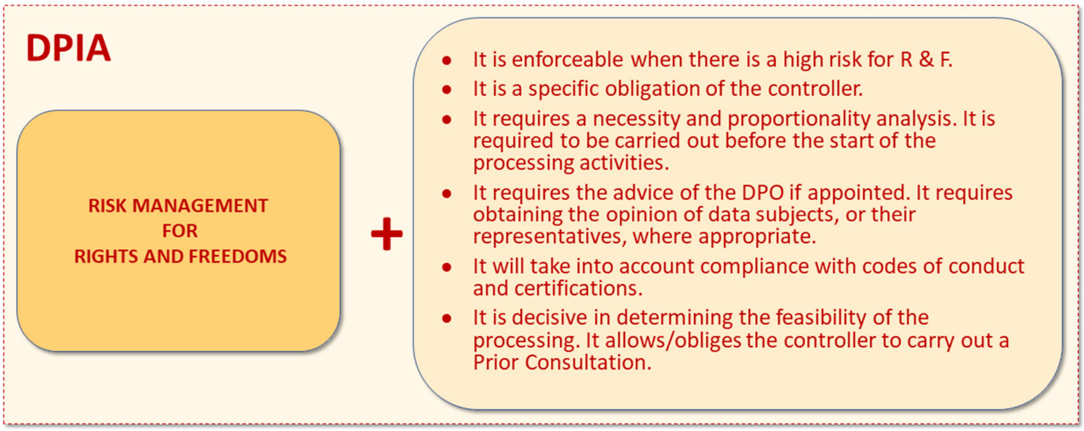
The features that the DPIA incorporates in relation to general risk management for rights and freedoms are:

- It is enforceable when there is a high risk to the rights and freedoms.
- It is a specific obligation of the controller.
- It requires an analysis of the necessity and proportionality of the processing[40] in relation to its purposes.
- It requires this to be done prior to the start of the processing activities[41].
- It seeks advice from the DPO if appointed.

[40] The "necessity analysis" of carrying out a DPIA should not be confused with the "necessity analysis of the processing" that is a requirement that the GDPR requires of the data controller in Article 35(7)(b).

[41] With some nuances that are developed in the section of the document dedicated specifically to the DPIA.

- It requires obtaining the opinion of the data subjects, or their representatives, where appropriate, in the risk management process[42], justifying, where appropriate, the inappropriateness or limitation in the disclosure of information.
- It shall take into account compliance with the approved codes of conduct referred to in Article 40 to which the controller has adhered.
- It shall take into account the requirements of the certifications applicable to the processing at the level of the controller.
- Their outcome should be taken into account in assessing the feasibility or unfeasibility of the processing from a data protection point of view. The DPIA is a tool to inform the decision making of the controller in relation to whether or not to carry out the processing activity or, where appropriate, to modify the processing within the parameters of the data protection principles.
- If necessary, depending on the level of residual risk, it obliges the controller to carry out a Prior Consultation (Art. 36) with the Supervisory Authority.



DPIA

RISK MANAGEMENT FOR RIGHTS AND FREEDOMS

+

- It is enforceable when there is a high risk for R & F.
- It is a specific obligation of the controller.
- It requires a necessity and proportionality analysis. It is required to be carried out before the start of the processing activities.
- It requires the advice of the DPO if appointed. It requires obtaining the opinion of data subjects, or their representatives, where appropriate.
- It will take into account compliance with codes of conduct and certifications.
- It is decisive in determining the feasibility of the processing. It allows/obliges the controller to carry out a Prior Consultation.

Figure 8: What the DPIA adds to the risk management process.

4. The DPIA as a tool for demonstrating compliance

In the WP248 Guidelines, along with the definition of DPIA, it is interpreted:

> *"DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation."*

Thus, one of the possible measures of *accountability* or demonstrating compliance is to conduct a DPIA, where this is not mandatory.

[42] Article 35.9 of the GDPR.

III. MANAGEMENT PROCESS OF THE RISKS TO THE RIGHTS AND FREEDOMS

A. PRECISE DETERMINATION OF THE PURPOSES OF THE PROCESSING

In order to carry out proper risk management, it is first necessary to identify and characterise precisely the purposes of the processing.

The purposes of the processing, as well as its legitimacy, must already be established before the start of risk management. This determination is a prior task that will need to be set out at this point in the analysis, and detailing how the controller has ensured that they have been correctly identified. In order to ensure that the purposes of processing have been correctly identified, the following properties must be complied with[43]:

Ultimate	The ultimate goal of the processing must be determined and not confused with intermediate goals, instrumental means or processing operations that take place at some stage of the processing or that may be dependent on the form of implementing the processing [44].
Specific	Sufficiently precise and concrete, specifying gaps, demands, requirements, obligations or opportunities objective and final objectives that the end of the processing comes to resolve or to respond to.
Measurable	They must define a desirable future state in qualitative terms.
Achievable and realistic	Guarantees are determined in order to achieve the purposes of the processing to the extent that it is possible to "demonstrate" that the ultimate goal will be achieved.
Limited	The purposes are to be achieved over a period of time and within a given stage of the processing lifecycle.

Table 3 Properties to be met by Well-Defined Processing Purposes.

In some cases, the purposes of processing may be confused with some of the measures that could be taken to achieve those purposes. For example, in processing for the purpose of personal security, access control or compliance, technical methods (such as video surveillance) or coercive methods (such as sanctions) may be used as measures to achieve this purpose. Video-surveillance operations or sanctioning processes are technical or organisational means used in a particular way to understand the implementation of processing. The use of such methods is not the ultimate goal of the processing, but they pursue intermediate objectives or are instrumental means to achieve the ultimate goal of the processing.

[43] Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final, http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf

[44] In case it is used in a processing, e.g. video surveillance, it does not imply that the purpose of the processing is video surveillance. The purpose could be to preserve the security of persons, to control access to an enclosure or any other purpose. Video surveillance operations are a means and a concrete implementation of such processing aimed at achieving this end.

The purposes of processing should be described in a clear, precise and understandable, but not simplifying, manner.

B. DESCRIPTION OF THE PROCESSING

In order to manage the risks to the rights and freedoms posed by a given processing operation, it is necessary to know about it and, to do so, it is necessary to analyse it. To analyse means to examine in detail, separating and considering independently each of its parts, in order to know their characteristics, qualities, restrictions and limitations, and thus to be able to draw conclusions.

The depth of this analysis must be sufficient to be able to reach conclusions regarding the risk to rights and freedoms and, furthermore, to comply with the obligations of the Records of Processing Activities. Normally, as it becomes clear that the risk may be high, the description needs to be revised downwards and made more detailed, so it will be an iterative process throughout the processing lifecycle.

PURPOSE OF THE PROCESSING OPERATION			
Its purpose	**Its nature**	**Its scope**	**Its context**
• Ultimate purposes. • Instrumental purposes. • Secondary purposes. • Other.	• The stages at which it is implemented. • The flow of personal data. • The processing operations required (manual and automated). • The assets/elements on which it is implemented. • The roles accessing the data. • The relevant technological features. • The involvement of processors in various operations. • Other.	• The extent of the amount of data. • The extent of the number of subjects affected. • The extent of data types and categories. • The geographical extent. • The extent of time of processing. • The extent in time of conservation. • The frequency of collection. • Granularity. • Other.	• The market or sector in which it operates. • The social environment in which it is deployed. • The regulatory environment. • The interaction with other processing of the entity. • The transfers of data that are necessary. • The international transfers involved. • The data breaches or incidents that occur in related processing. • The collateral effects on society • Other..

Table 4 Example of Information describing the Processing that is Useful for Risk Management.

The processing study could be carried out at different levels of detail (detailed in the chapter "Description and Contextualisation of the Processing"):

- High-Level Processing Study.
- Analysis of the Processing Phases.
- Analysis of Data Lifecycle.
- Inventory of Assets.
- Description of use cases.

The description of the processing may go beyond the established regulatory obligations to draw up and maintain a Records of Processing Activities with the minimum content required by Article 30 of the GDPR and Article 31 of the LOPDGDD. However, it has to be integrated with the solution adopted in the organisation to implement the registration process and, in general, to manage the organisation's processes.

As a potential source of risk, knowledge of the technologies to be used, as well as their associated risks, must be understood as an obligation of the data controller and part of his or her duty of care in relation to compliance with the provisions of the GDPR. In no case can ignorance of the technological context be understood as an exemption from the obligations of the controller.

Likewise, when, within the framework of the risk management process, prior consultation of the Supervisory Authority referred to in Article 36 of the GDPR is necessary, this consultation shall not include the analysis of those products, services and systems existing on the market that could be used, as well as the risks associated with them according to the technologies they incorporate. The process of identifying these risks is part of the duties of the controller and is part of the advisory functions of the DPO.

C. THE ASSESSMENT OF THE LEVEL OF RISK RELATED TO THE PROCESSING FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

The assessment of the level of risk has two objectives. The first is to optimise efforts to mitigate and manage risks in a proportionate manner. The second is to determine whether the level of risk requires compliance with Articles 35 and 36 of the GDPR (high-risk scenarios).

1. Risk assessment process

The process of assessing the level of risk is a discipline with a well-established methodology common to any risk management process. The following tasks must be carried out to assess the level of risk associated with a processing:

- Identify risk factors or threats[45] to rights and freedoms.
- Analyse them, in terms of their impact and likelihood, in order to be able to carry out the assessment of the level of inherent risk arising from each of the risk factors.
- Assess the overall level of risk of the processing to the rights and freedoms of the data subject.

A risk or threat factor can be defined as a potential cause of harm to the rights and freedoms of natural persons. Risk factors can originate from the processing itself, such as the purpose of the processing, the processing operations, the technology used, etc. They can also originate from side effects and undesirable effects arising from the context internal or external to the organisation. Every risk factor has a level of potential impact on data subjects. In addition, there will be a certain likelihood that such a factor of risk actually materialises. The likelihood will depend both on factors internal to the processing and external (contextual) factors.

[45] In this text, the term "risk factor" will be used as a synonym for "threat". "Threat" is a well-defined term in risk management literature, and in that literature "risk" is derived from the likely materialisation of a threat with a given impact. However, since the GDPR and its implementation use the term "risk" as a synonym for "threat", the latter will be used.

2. Inherent Risk and Residual Risk

Inherent risk is the result of assessing the level of risk **prior** to the implementation of measures and safeguards to reduce the risk arising from each of the risk factors. This involves considering the joint effect of all possible risk factors in the possible scenarios in which they could materialise with a given likelihood producing a given impact. All of them need to be assessed together, taking into account their cumulative action and their combined effect.

The residual risk is the result of assessing the resulting level of risk **after** taking measures and safeguards to reduce the risk arising from each of the risk sources. The objective is that the residual risk is reduced to an acceptable level of risk.

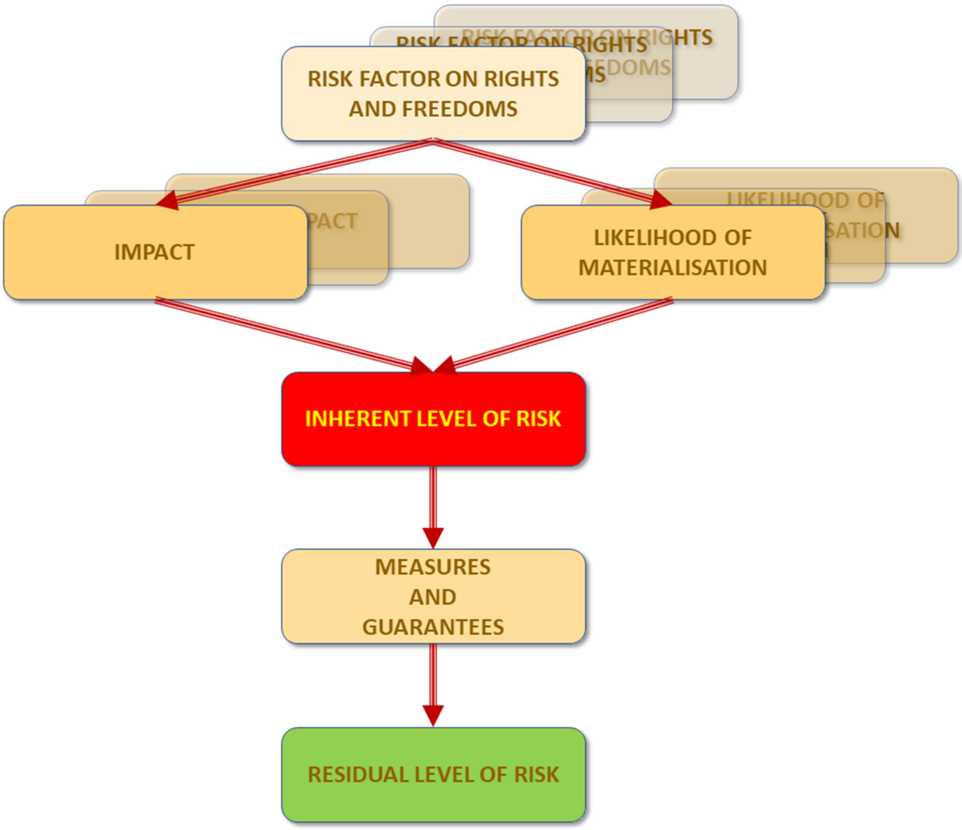


Figure 9: Inherent and residual risk assessment

3. Identification of risk factors

Identifying a risk factor consists of detecting the source of an event that may have an impact on the rights and freedoms of data subjects.

The legislation prior to the GDPR, in particular Title VIII of the regulation approved by R.D. 1720/2007, which has now been superseded, carried out an assessment of the level of risk of the personal data files in relation to data security and not in relation to the rights and freedoms of natural persons. This analysis had the following limitations:

- It was file-oriented, not processing-oriented.
- It was primarily based on the categories of data used[46].
- It was aimed solely at determining security measures.
- It had been made by the legislator.
- The security measures were a list of minimums, which was understood by many controllers as a closed list.

However, the current context is much more complex and such a simplified model does not provide an answer to current situations[47]. Therefore, the GDPR requires that:

- The assessment of the level of risk is a task of the controller, which should be oriented towards the processing operations it carries out and not towards the possible content of a data file.
- The assessment of the level of risk takes into account all aspects of the processing, which arise from the nature, scope, context, and purposes of the processing.
- The measures and safeguards to be adopted should not be limited to security measures, but should also include measures on the design of the processing, data protection governance and policies, data protection measures by design (unlinkability[48], transparency and control), management of personal data breaches and, where appropriate, carry out a DPIA.

4. Identification of risk factors for the processing of personal data in the regulation

Specific risk factors are identified in the GDPR, and in its development through other standards, the EDPB guidelines and the AEPD. In addition, in certain cases, the impact and likelihood of these are set by default, thus facilitating the analysis for the controller. Examples include the following:

- The WP248 Guidelines state that:

  > *For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.*

  The existence of an IoT application in processing is a risk factor to be managed. The controller has to assess the impact it may have on rights and freedoms taking into account the certainty that such a risk factor is materialised in the processing.

- Article 35(3)(a) states that processing is high risk if it includes:

  > *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on*

[46] Certain purposes and sectors of activity were also taken into account.

[47] Recitals 7 and 9 GDPR.

[48] Unlinkability: seeks to process data in such a manner that the personal data within a domain cannot be linked to the personal data in a different domain, or that establishing such a link involves a disproportionate amount of effort.

which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

The following risk factors are identified in the above paragraph:

- Techniques relating to the nature of the processing: automated processing and profiling.
- Types of data relating to the nature of the processing: personal aspects.
- Extension of the scope of processing: systematic and comprehensive assessment.
- Purposes of processing: decision making with legal or similar effects.

When all these factors are combined, the impact on rights and freedoms is high risk and the GDPR requires a DPIA. In order to manage this risk, measures and safeguards should be identified to mitigate the risk associated with these factors.

Conversely, if not all of the above factors were present in the processing, but only a subset of them, the processing would have a certain level of risk without being "high risk". This level of risk is determined by the risk factors involved in the processing. In addition, the measures identified above would be valid for managing such risk, taking into account the factors that are present.

- On the other hand, Article 28.2.b of the LOPDGDD establishes that high risk must be considered in the following case:

  Where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data.

  Therefore, in this case, it is necessary to determine the likelihood that an erosion of the rights of individuals, or a lack of control over their personal data, will materialise in the processing. In addition, the impact should be estimated according to other processing circumstances.

  From the above examples we can conclude that, both in the GDPR and in its development, risk factors that need to be managed are already identified, some of them with a high impact and total likelihood, and others where the impact they could produce and/or the likelihood of their materialisation needs to be estimated.

Therefore, in the task of identifying sources of risk, the controller or processor does not have to start from scratch, but the GDPR and its developing regulations have already identified specific sources of risk in:

- The cases in article. 35.3 of the GDPR.
- Special regulation that requires a DPIA for processing or identifies risk factors.
- Cases and examples from the WP248 Guidelines.
- Cases on the list approved by the AEPD on the basis of article 35.4 of the GDPR.
- Cases under article 28.2 of Organic Act 3/2018, of 5 December, on Protection of personal data and guarantee of digital rights (LOPDGDD).
- Cases under Article 32.2 of the GDPR.

- The risks identified in Recital 75[49].
- The specific cases and conditions described in the guidelines published by the EDPB for specific processing.
- The specific cases and conditions described in the codes of conduct in accordance with Article 40 and certification mechanisms in accordance with Article 42 of the GDPR.

To facilitate this task, the chapter "Identification and analysis of risk factors" in section 2 lists all the factors that have been identified in the various texts listed above.

5. Very high impact risks

Setting a predetermined level of measures and safeguards for a risk factor based on the likelihood of its materialisation may be a mistake, especially in cases where the impact may be of very high intensity. If the impact of a risk factor is very high for the rights and freedoms of individuals, even if the likelihood of its materialisation is very low or negligible, the risk factor needs to be properly managed.

Much of the compliance and processing guarantees are based on the framework established by the rule of law, the social, political, and economic situation and the state of the art. These foundations are normally considered to be "default" and immovable in the medium term. Moreover, they are often beyond the control of the controller. Such safeguards usually support the principles of restriction of processing, and relate to legal, organisational, and technical aspects.

Low likelihood scenarios, but which may compromise such basic safeguards, could be the publication of regulations that radically alter legal safeguards (e.g. the PatriotAct or the CloudAct), disruptive technological developments (e.g. quantum computing, advances in cryptanalysis), radical changes in international relations (e.g. Brexit), situations of special emergency (e.g. armed conflicts, pandemics), breakdown of the rule of law (e.g. states of emergency, subversion of constitutional order), etc.

This assessment is not necessary for all processing, but only for those which, due to their extent or intrusiveness, could be very high risk. Massive data processing, namely special categories, extended in time and with consequences on rights and freedoms would be candidates for this analysis. Some cases could be found in the processing of public administrations, large telecommunications companies, large financial institutions, insurance companies, health services, large Internet services, etc

[49] The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

D. RISK MANAGEMENT

Dealing with risk involves **taking measures and implementing safeguards** that specifically diminish the level of risk to rights and freedoms. This task involves going beyond mere declarations or apparent commitments. It involves implementing actions to reduce, eliminate or manage identified risks. Addressing risks means reducing the potential for harm by reducing either the likelihood of them materialising or the impact they represent. This task, as part of risk management, has to be performed irrespective of whether the processing is high risk or not.

In risk management terminology, "risk management" refers to the selection of measures and safeguards to reduce, eliminate or assume in a controlled way the identified risks. In the context of data protection, the correct way to express it would be "risk management related to the processing". As it could be confusing, the expressions "attend to", "diminish", "deal with" or "take care of" will be used interchangeably throughout the text.

Measures and safeguards that aim to address or mitigate risk in processing are often referred to as "controls" in risk management terminology.

The GDPR already outlines some safeguards to be implemented in case of a high risk to rights and freedoms. These are, for example, the timeliness of the implementation of data protection policies (Art. 24.2), or the obligation to communicate a personal data breach to data subjects (Art. 34), among others.

Addressing processing risk factors is an iterative process that takes place primarily during the conception and design stages of the processing lifecycle. In each iteration, controls shall be applied to reduce the likelihood or impact of the identified risk factors and the residual risk shall be reassessed as many times as may be necessary until an acceptable level of risk is reached. Control measures should be considered separately for each identified risk, even if their combined effect is later assessed, and as many control measures as necessary should be established until an acceptable level of risk is achieved.

Controls derived from risk management can be applied to multiple processing operations that are similar. Some of the controls could also be part of the controls applied from other data protection strategies of an organisation such as: data protection policies of the controller, data protection policies by design and by default or security policies by design and by default.

1. Classification of measures and guarantees

The measures that can be taken to mitigate risk could be classified, following the risk management literature, according to different criteria:

- Insofar as they prevent the materialisation of risk or are activated in response to a materialised risk, they can be classified into proactive/preventive, detection and reactive/corrective measures.
- On the strategy of how to deal with risk, we distinguish between measures aimed at:
    - Reduce/mitigate risk: To reduce the level of risk, control measures should be put in place to reduce the likelihood levels and/or impacts associated with the inherent risk.
    - Avoid/eliminate risk: If the risk is very high and you do not want to bear it, you may decide to stop the processing activity or, alternatively, to modify the nature, scope, context and purpose of the processing in order to avoid the risk.
    - Accept/assume the risk: If the inherent risk is below the level of risk considered acceptable, it can be assumed, but it is important to continue to manage it on an ongoing basis.
- Depending on their nature, controls may incorporate measures:
    - Organisational Measures: Measures associated with the procedures, organisation and/or governance of the entity related to the implementation of data protection policies.
    - Legal Measures: Legal safeguards that may be necessary, such as the establishment of confidentiality clauses or the adoption of non-re-identification undertakings, among others.
    - Technical Measures: Protection measures by design, security measures or measures for automatic accountability, among others.

Management of the Risks posed to Rights and Freedoms.				
Proactive/ preventive	Legal safeguards	Technical safeguards	Organisational safeguards	Reduce/ mitigate
Detection				Avoid/eliminate
Reactive/ corrective				Accept/ assume

Table 5 Classification of Risk Management Measures and Safeguards

Based on the proactive accountability model set out in Chapter IV of the GDPR, the measures and safeguards that can be adopted to mitigate data protection risks can be classified as follows:

Measures and safeguards based on the GDPR	Measures on processing concept and design.
	Governance and policy measures
	Data protection measures by default[50] and by design
	Personal data breach prevention and management measures / security measures.

Table 6 Measures and Safeguards for Risk Management based on the GDPR

The control measures taken must be associated with each of the risk factors identified. It is very important to ensure that the allocation of controls is appropriate and commensurate with the risk, and that risks are managed together, taking into account the interrelationship between them, with the clear objective of being able to mitigate the risk levels of the processing as a whole.

The result of addressing the risks is the residual risk, defined as the level of risk resulting from the processing once control measures have been implemented to mitigate and/or reduce the level of exposure in relation to the set of risk factors identified. In contrast to inherent risk, residual risk refers to the control measures defined on the processing.

2. Transparency and Rights as Risk Reduction Measures

Chapter III of the GDPR establishes obligations of transparency and information, and determines a set of rights that the data controller must provide to data subjects under a series of minimum conditions. Recital 60 interprets these duties as extending to the extent necessary to ensure fair and transparent processing[51]. These obligations are part of the controller's compliance requirements and are not measures to mitigate the risk of the processing.

However, transparency and information measures going beyond the above may be put in place to mitigate the risks of processing. Once the obligations of fairness and transparency are fulfilled, one can, for example, make explicit to the data subject ways of preventing the risks incurred by the processing, by publishing relevant information on the DPIA or by detailing the types of data collected, which could in certain cases be a measure to reduce the risk of the processing.

In the same vein, addressing the rights of data subjects by ensuring diligence that goes beyond the provisions of Article 12 of the GDPR, e.g. in terms of time, means and channels, could be a way of reducing certain risks in some processing operations.

[50] It should be remembered that data protection measures have to be implemented by default, i.e. in any case and irrespective of the risk. See Guide to Data Protection by Default.

[51] Recital 60. The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed.

E. PERSONAL DATA BREACHES AND SECURITY IN PROCESSING

All processing will be implemented on an information system, which will be partly automated and partly manual. In addition to the risk to rights and freedoms that the existence of such processing may pose in itself, it is mandatory to determine also the risk to those same rights and freedoms that a personal data breach, i.e. an unauthorised or accidental processing of data, may materialise[52].

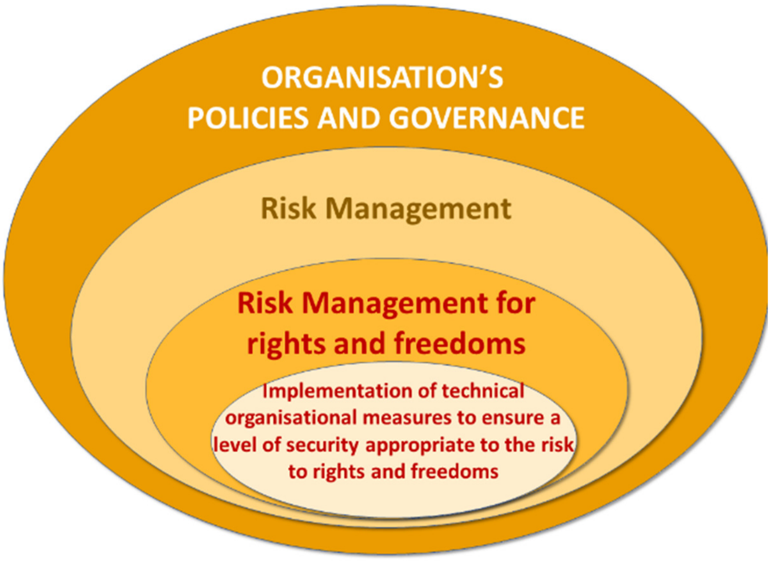

ORGANISATION'S
POLICIES AND GOVERNANCE
Risk Management
Risk Management for rights and freedoms
Implementation of technical organisational measures to ensure a level of security appropriate to the risk to rights and freedoms

Figure 10 Security Management as a part of Risk Management for Rights and Freedoms.

As the WP218 Statement interprets, it has to be underlined that addressing the risks that a data processing might entail for the rights and freedoms of individuals cannot be limited to the application of security measures alone. Therefore, security risk management is one of the activities for the management of risks to rights and freedoms and has to be subordinated to the latter. In addition, from a GDPR perspective, mitigation measures should aim to reduce the impact and likelihood of personal data breaches affecting the data subject.

[52] Recital 85: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned"

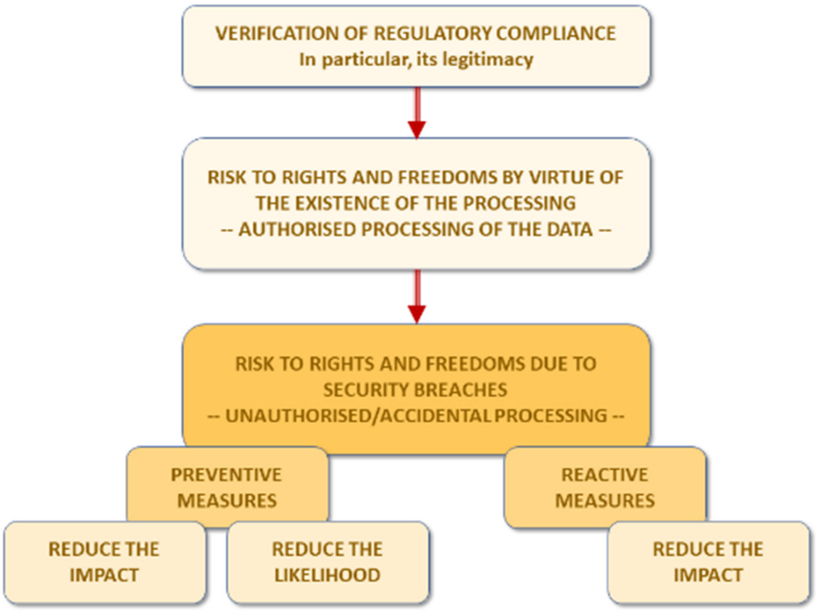

VERIFICATION OF REGULATORY COMPLIANCE
In particular, its legitimacy
RISK TO RIGHTS AND FREEDOMS BY VIRTUE OF THE EXISTENCE OF THE PROCESSING
-- AUTHORISED PROCESSING OF THE DATA --
RISK TO RIGHTS AND FREEDOMS DUE TO SECURITY BREACHES
-- UNAUTHORISED/ACCIDENTAL PROCESSING --
PREVENTIVE MEASURES
REACTIVE MEASURES
REDUCE THE IMPACT
REDUCE THE LIKELIHOOD
REDUCE THE IMPACT

Figure 11: Security Measures in the Management of Risk to Rights and Freedoms.

1. Data Protection by Default

The document "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"[53] of the European Data Protection Board, in its paragraph 47, states that security measures should always be included by default:

> *Information security shall always be a default for all systems, transfers, solutions and options when processing personal data.*

This means that, even if the risk of the processing to rights and freedoms is low[54], the controller or processor:

- It cannot ignore the establishment of security measures, which have to be implemented regardless of whether the processing is low risk or not.
- When choosing the specific security measures to be implemented, the process of selecting each one of them must be guided by an analysis of risks to the rights and freedoms of natural persons.
- In the case of processing operations with a risk above an acceptable level, security measures should be employed to reduce the level of risk of the processing.

2. Scope of Security Measures

In relation to such measures, section two of chapter four of the GDPR is devoted to the security of personal data. In particular, Article 32 is

[53] Published in draft version at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en

[54] The risk associated with processing, however low, will never be zero.

devoted to measures to ensure the security of processing and Articles 33 and 34 on specific contingency measures in the event of a personal data breach. In other words, the GDPR provides for both preventive (to avoid) and corrective (to react to the materialisation of a risk) measures.

In this regard, Article 32.155 specifically lists a non-exhaustive set of security measures that could be envisaged for a processing operation, such as:

1. Those aimed at ensuring confidentiality, integrity, and availability.
2. Those aimed at ensuring the resilience[56] of processing systems and services and providing the ability to restore availability and access to personal data quickly in the event of a physical or technical incident.
3. The pseudonymisation and encryption of personal data.
4. Processes for regularly testing, assessing and evaluating the effectiveness of security measures.

From Article 32.1 it is concluded that the impact on rights and freedoms of an incident affecting the information system must be determined, whether in relation to the materialisation of attacks, intrusions, or any kind of unauthorised processing. This impact must also be assessed for accidental incidents, both technological and human, and those associated with natural events. Similarly, the impact on rights and freedoms will need to be determined where the processing is not automated.

In addition, in this relationship, explicit reference is made to the need to manage possible errors or failures that may arise from the different technical and organisational measures that implement data protection strategies by default, from design or other safeguards (the systems of safeguards) such as:

- In the aforementioned pseudonymisation and encryption of personal data.
- On anonymisation processes.
- In data unlinkability processes.
- On the execution of data deletion.
- In the implementation of federated processing.
- In the application of data protection measures by default.
- Etc.

[55] 32.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
the pseudonymisation and encryption of personal data;
the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

[56] Resilience is the ability of a system to continue to provide service in the face of an unforeseen event, albeit with a loss of effectiveness or efficiency. While availability is a ratio of the days the system provides service to the days it does not provide service. For example, a server with 99.9% availability informs us that it will be down for 8.7 hours on average per year.

Finally, it is necessary to manage technical errors arising from the automated implementation of personal data processing that may result from, for example:

- Automatic decision systems.
- Decision support systems.
- Biometric processing.
- Errors in the synchronisation of transactional systems.
- Errors in the separation of virtual environments.
- Etc.

The above failures and errors can lead to specific problems of confidentiality, integrity, availability, traceability, or authentication, but also to other more specific problems such as data quality, discrimination, etc. Moreover, practical experience shows that the estimation of the impact of these failures and errors on personal data is often not taken into account. It is therefore deemed necessary that they be considered in a unique way when analysing the risk to rights and freedoms.

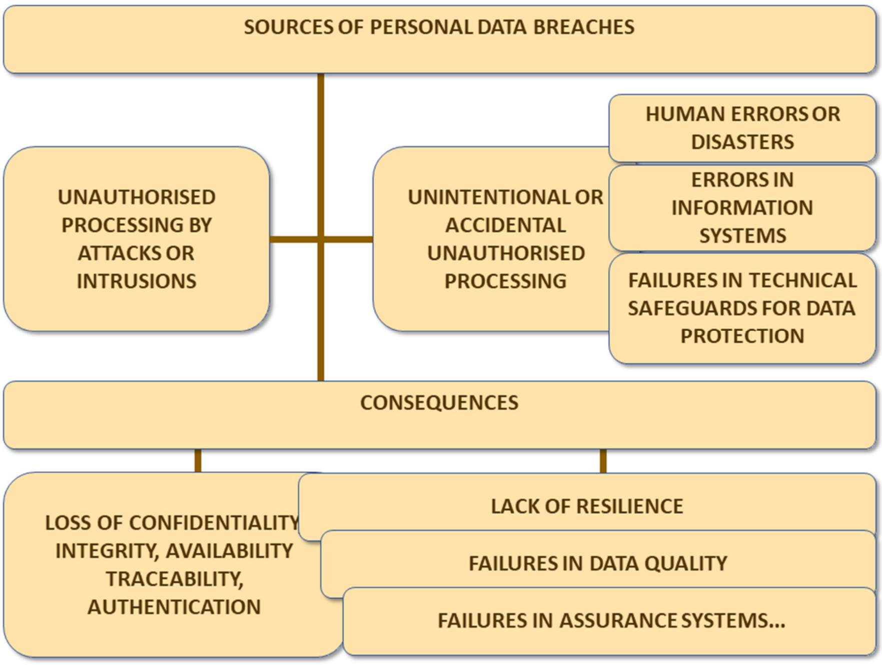

SOURCES OF PERSONAL DATA BREACHES
UNAUTHORISED PROCESSING BY ATTACKS OR INTRUSIONS
UNINTENTIONAL OR ACCIDENTAL UNAUTHORISED PROCESSING
HUMAN ERRORS OR DISASTERS
ERRORS IN INFORMATION SYSTEMS
FAILURES IN TECHNICAL SAFEGUARDS FOR DATA PROTECTION
CONSEQUENCES
LOSS OF CONFIDENTIALITY INTEGRITY, AVAILABILITY TRACEABILITY, AUTHENTICATION
LACK OF RESILIENCE
FAILURES IN DATA QUALITY
FAILURES IN ASSURANCE SYSTEMS...

Figure 12: Sources of Personal Data Breaches

3. Estimating the Level of Risk of a Personal Data Breach

In order to estimate the potential impact of a personal data breach, it is necessary to consider the consequences of the breach materialising. One way to do this is to consider the possible scenarios for the materialisation of a breach, determine its consequences, and assess how it affects the rights and freedoms of data subjects, especially if the consequences are irreversible.

In the face of such consequences, measures must be identified to reduce the likelihood of the breach occurring. Given that the likelihood of the breach materialising always exists, measures must also be considered to eliminate, diminish or reverse its consequences on the person concerned.

Let's look at a simplified example. Consider the framework of home automation or consumption control applications that could capture the domestic activity of individuals. In this case, several breach scenarios should be envisaged, one of which could be the following:

Processing based on home automation or consumption control applications	**Scenario 1**
Breach materialised:	Confidentiality: access to the records of activity of the users of the home automation systems that are stored on a central server.
Compromised data:	Basic data, contact data, detailed data on system events, usage or consumption per minute over a long period of time.
Damage to the data subject:	The user's address and identification details are known. It could be inferred when the household is empty. The times of entry and exit from the household could be inferred. It could be inferred whether the individual lives alone or in company. It could be inferred when they go to sleep. Very personal aspects, and even special categories of data, can be inferred. Etc.
Assessment of the impact on the data subject:	It can have a very significant impact, affecting fundamental rights and freedoms in an irreversible way.
Measures to reduce the impact:	Reduce the temporal precision of data collection, and instead of collecting data by the minute, collect data by hours, days, or weeks (reduce granularity) Group data from different individuals (increase aggregation). Reduce the dataset collected (data minimisation). Delete individually collected information in a very short space of time, almost real time (data storage). Have a very rapid procedure for communicating to those affected (data breach disclosure). Etc.
Measures to reduce the likelihood:	Identification measure for access to the system. Data access control systems. Encrypt information in transit and at rest. Etc.

Table 7 Example: Personal Data Breach Scenario

The following reflections can be drawn from the above example:

- Scenarios should be considered for cases of loss of confidentiality, availability, integrity, authentication, traceability, resilience, failure of safeguards (such as re-identification in anonymised or pseudonymised data), errors in processing or any other as deemed appropriate.
- In addition to measures that reduce the likelihood, it is necessary to implement measures that reduce the impact of a breach, as the likelihood of a breach occurring is never zero.
- Measures that reduce the impact are, in many cases, privacy by design and/or by default.
- There are measures that are preventive, e.g. applying data aggregation policies, and others that are reactive, e.g. having a breach management system in place that allows for swift communication to those affected.
- In risk assessment, it is necessary to evaluate what impact it may have on the individual and on society, as there are breachs whose social impact makes it more difficult to minimise risks. In the example shown above, if the breach affects a single individual, reactive mechanisms can be put in place that are unfeasible if thousands of users are affected.

Therefore, without prejudice to other steps and measures taken, the assessment of the risk to rights and freedoms is not covered by the assessment of the impact of an incident on the organisation alone. Moreover, the adoption of security measures has to be carried out under a vision of risk management for rights and freedoms that goes beyond the strict scope of the organisation. In other words, the analysis cannot only focus on the impact of the incident on the relationship of the data subject with the entity, as situations such as, for example, the following could occur:

- A loss of confidentiality in Entity-A can lead to identity theft of a subject. Such impersonation can be used on Entity-B to access the data subject's data.
- Tampering with the integrity of a person's data in an A-Entity may prevent that person from accessing services provided by a B-Entity.

4. The likelihood of a personal data breach

In order to determine the level of risk, it is necessary to determine the likelihood of the risk materialising. At this point, we have to face the reality that the security incident logs show us every day, which is as follows: Systems fail. There are no 100% secure systems. Therefore, processing cannot be approached under the assumption that security will never be breached.

Moreover, when the period of time in which the processing will be active (processing lifecycle) tends to be infinite, a personal data breach is only a matter of time:

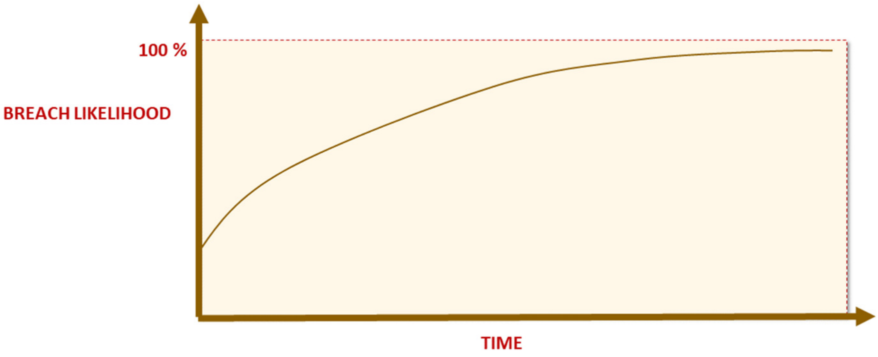


Figure 13: Evolution of the likelihood of a breach over time

The likelihood of a breach materialising is never zero, and the more time elapses, the greater the chance of an incident occurring. Therefore, when assessing the likelihood, it is necessary to take into account the length of time the processing in question is intended to be active.

5. Resilience

Article 32(1) of the GDPR requires both availability and resilience, concepts that may be related, but are distinct. Availability is the property of an asset to be accessible and usable on demand by an authorised entity[57].

The term resilience refers to the ability of an organism, organisation, system or society to adapt to change without altering its basic structural and functional characteristics. They have to adapt without reaching breaking point, paralysis or crisis. After such adaptation, the entity may return to its original state or even have improved its suitability to the environment. This means the ability to assume, with flexibility, limiting situations and to overcome them.

Organisational resilience studies resilience in organisations. To achieve this, the organisation must anticipate, prepare, respond and adapt to changes or events that may occur. These can be changes in the economic, political, legal, social, environmental, etc. context; as well as damage to infrastructure, acts of terrorism, cybercrime, etc.

Resilience is inherent, relative and no organisation, network or system can be fully resilient. The degree of resilience will depend on:

[57] Definition in ISO-27001

People capability	Staff, from the highest to the lowest level, must have the ability to detect change, the ability to communicate change, the ability to understand change, the ability to innovate in the face of change, the ability to act and the willingness to act proactively, in real time.
Adequate flow of information	It must be agile, specific, minimal, complete and from and to the adequate people .
Leadership	There must be clear decision-making points with responsibilities and accountabilities that are well defined.
Strategic adaptability	Physical, technological and organisational structures need to be able to evolve in real time towards new objectives or ways of acting.

Table 8 Factors that determine the Degree of Resilience of an Organisation

Organisational resilience, like all security measures, relies fundamentally on people. Resilience must allow for adaptation at the necessary speed, taking a holistic view of the connectivity of all events occurring in the internal and external context of the organisation. Resilience must therefore be embedded throughout the organisation.

Resilience and sustainability are related but distinct concepts. Resilience is linked to an organisation's preparedness to react to a changing context. The sustainability of the organisation is related to actions to avoid or mitigate its impacts inside and outside the company, on its environment, ensuring its own long-term viability, and to contribute, in turn, to that of the environment.

6. Integration of risk management requirements for rights and freedoms into the ISMS

Information security management is a very mature discipline, with well known and implemented management models (ISMS or Information Security Management System) and guidelines (ISO 27000 or ENS standards) that can be considered as security standards.

Information systems are a projection of the entity's processing, as they are the means that support it and, therefore, information systems policies should be a projection of the entity's information policies. In turn, security policies are a subset of the entity's information policies.

The design, maintenance and operation of information systems, manual and automated, is feeded by a set of functional and non-functional requirements. One of these non-functional requirements are the security requirements, which are in line with the entity's objectives and which, in turn, translate into specific information system security requirements.

However, in organisations where management levels were poor, information systems policies have been the driving force behind the organisation's processes. The very nature of these requires a systematised approach to processing implementation. Thus, in some organisations, the information systems policies that emerged from ICT departments made up for the lack of information policies and quality policies in the organisation.

This reactive, bottom-up approach is contrary to the proactive accountability model, where decisions have to be taken from the top down, from the design of processing in the organisation and with a holistic view. Moreover, this approach has had negative consequences, for example, forcing information systems administrators to make decisions without clear guidelines and communication channels to convey the final requirements of the entity's processes, business policies, effectiveness, and efficiency criteria. Information systems administrators should implement the security requirements provided by the security officer with a holistic view of the organisation but should not carry out security-related decision-making beyond the technical and operational issues related to the administration of the systems themselves.

In particular, the set of security requirements, in relation to rights and freedoms, has to be one of the inputs to the overall risk analysis process of information systems that has to reach the ICT department.

Non-functional security requirements may stem from different objectives of the entity in general and from the data processing in particular: security of persons, theft, fraud, etc. In turn, it will be necessary to take into account other functional and non-functional requirements, in addition to those arising from regulations, contractual obligations, certifications, etc.

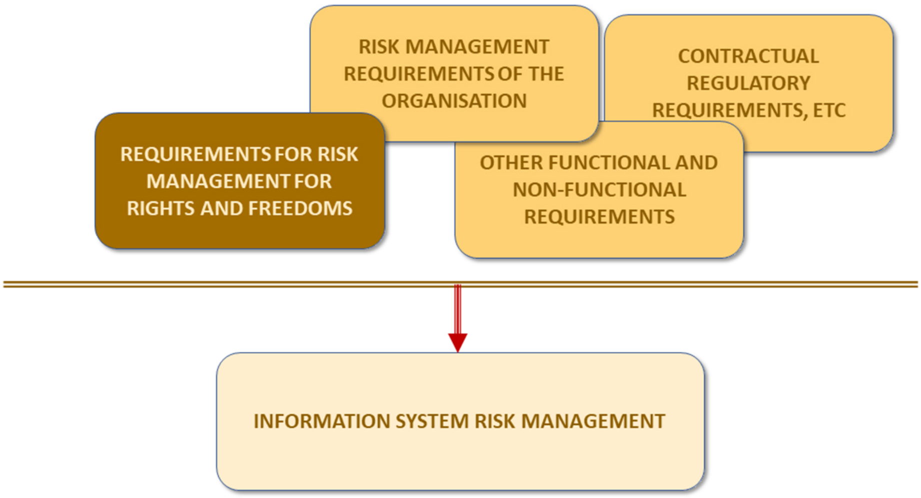

RISK MANAGEMENT REQUIREMENTS OF THE ORGANISATION
CONTRACTUAL REGULATORY REQUIREMENTS, ETC
REQUIREMENTS FOR RISK MANAGEMENT FOR RIGHTS AND FREEDOMS
OTHER FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS
INFORMATION SYSTEM RISK MANAGEMENT

Figure 14: Integration of Security Requirements for the Protection of the Rights and Freedoms

The way in which these requirements are implemented has to be balanced between the different objectives. For example, if, in order to protect the safety of persons, a solution based on biometric identification is proposed. It has to be assessed that it may clash with data protection or with the image the company wants to provide. Another example could be, in order to avoid fraud, the implementation of authentication procedures that are so robust that they collide with sales strategies and product accessibility.

7. Measures to manage personal data breaches.

Incident management is one of the specific security control objectives. The GDPR dedicates two articles, 33 and 34, and three recitals, 85, 86 and 88, to this objective, where it establishes obligations on data controllers in relation to the notification of personal data breaches to the supervisory authority and the communication of their occurrence to data subjects according to the risk to the rights and freedoms they represent.

Breach management is an obligation of the controller, which should include the establishment of preventive and reactive measures depending on the risk and which has an impact on the risk management cycle of the processing. That is to say, the controller must, in a preventive manner, implement mechanisms for detecting and managing breaches. The detection of a breach not only implies the use of technical means, but also that full information on the size and impact of the breach reaches the decision-making bodies who have to act on it in time.

In addition, before a personal data breach materialises, the controller must be prepared to meet at least the obligations arising from the regulation. The level of preparedness of the controller should be determined on the basis of the assessment of the risk posed by the occurrence of a personal data breach.

On the other hand, once the immediate actions to react to the breach have been completed, the controller will have to address, within the risk management cycle, all those measures that are necessary to prevent the incident[58] or breach from occurring again. This task will involve the review of the controls that were related to the occurrence of the breach, as well as the possible implementation of new controls that may be necessary.

On the contrary, the regulation establishes a series of obligations in the event of a data breach that do not depend on the performance of a risk analysis, such as, for example, the obligation of the processor to notify, without undue delay, the controller of personal data breaches affecting the processing operations (Art. 33.2) or the obligation of the controller to document any personal data breaches, including the facts related to the breach, its effects and the corrective measures taken (Art. 33.5).

Another obligation that does not depend on risk management is that the controller must be able to detect the materialisation of personal data breaches and shall be able to manage them in order to comply with the obligations of Articles 33 and 34.

[58] Article 35(5) of the GDPR obliges the controller to document or record any event related to a personal data breach, including the facts related to it. Any event or situation that may relate to a security breach to the extent that it could lead to or facilitate a security breach of personal data, regardless of whether it has resulted in damage to any of the security dimensions, should be considered a personal data security incident.

What does depend on risk management is the size of the technical and organisational measures for incident management, such as:

- Use of incident management tools adapted to the GDPR.
- Established procedures for compliance with the obligations relating to Articles 33 and 34 of the GDPR.
- Protocols for identifying additional risks generated by the breach and for reassessing the level of risk to the rights and freedoms of data subjects.
- Etc.

More information on the management of personal data protection breaches can be found in the following resources:

- Personal Data Breach Notification Guidance
- Tool for assessing the obligation to communicate to data subjects: COMUNICA-BRECHA RGPD
- Data breach notification form to the Supervisory authorities
- Microsite on personal data breaches

F. IMPLEMENTATION OF CONTROLS, VERIFICATION AND REASSESSMENT: RISK MANAGEMENT AS A CONTINUOUS PROCESS

Once the set of controls has been decided, they need to be deployed throughout the processing concept, design and implementation process, as well as in its evolution or when the need for processing revision is identified.

In risk management, it is necessary to continue to observe processing and audit its results on a regular basis in order to ensure that the effectiveness of the measures implemented is maintained, the results obtained are as expected[59] and the nature, scope, context and purposes have not been altered.

The verification of the correct application of measures and safeguards, as well as the review of the level of risk and its management, is a process to be carried out throughout the entire lifecycle of the processing. A verification process is recommended during the implementation phase in order to ensure and validate that the control measures defined in the Action Plan have been properly implemented.

The ideal scenario is that these tasks are generally integrated into the organisation's policies and procedures relating to the management of the processing lifecycle. In short, that they are reflected in a processing management action plan.

There are several references in the GDPR to this need to introduce risk management throughout the different stages of the processing lifecycle. Article 24

[59] Recital 74 "The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."

states that risk management measures "shall be reviewed and updated as necessary". Likewise, Article 25[60], which establishes Data Protection by Design and by Default, states that these measures shall apply "at the time of the determination of the means for processing and at the time of the processing itself". Article 32, on Security Measures, paragraph 1.d, establishes the obligation of "a process for regularly testing, assessing and evaluating". Finally, Article 35, on the DPIA, provides that the DPIA shall be carried out "prior to processing".

In this respect, the WP248 Guidelines state:

> *In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons".*

Note 10 of the same WP248 Guidelines states:

> *It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analysed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly.*

Risk management is therefore a continuous and cyclical process. This management has to make its first cycle with the first phases of the processing: before determining the means of the processing (in its conception, analysis, design, prototyping and implementation) and before executing the processing (testing and preparation/deployment). In addition, risk management needs to be repeated throughout the life cycle of the processing to assess and address changes that may occur in the subsequent phases (operation, maintenance, evolution and withdrawal).

[60] 1. Taking into account ... the risks of varying likelihood and severity represented by the processing to the rights and freedoms of natural persons, the controller shall implement, both at the time of the determination of the means of processing and at the time of the processing itself, appropriate technical and organisational measures, ..., and integrate the necessary safeguards in the processing ...

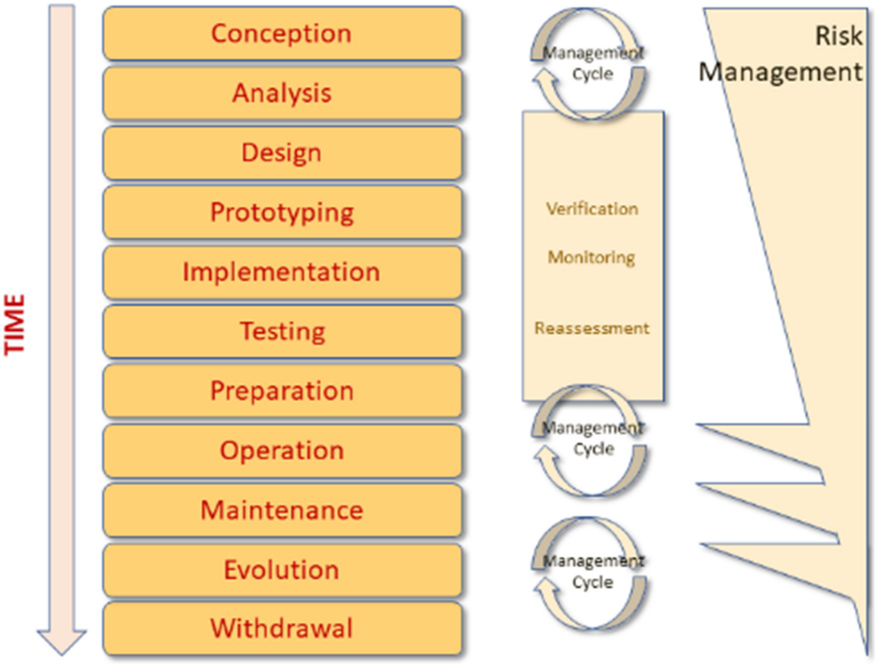


Figure 15: Risk management in the processing lifecycle

The figure is intended to give a generic overview of the effort that might be required for the different iterations of risk management throughout the processing lifecycle, with a few points to be made:

- Risk management has to be carried out, in a first iteration, in the conception of the processing.
- There are phases in which, *a priori*, the actions derived from risk management should be verified and, if necessary, re-evaluated, and where this activity could be more intense, such as the operation, maintenance and evolution phases.
- Risk reassessment can be triggered by events that are distinct from the processing phase of the processing lifecycle and depend on the context, i.e. events external to the processing.

With regard to verification and reassessment, as set out in Article 24, measures to achieve compliance with the GDPR must be guided by "the nature, scope, context and purposes of the processing", in addition to the risks. The processing activity may evolve through any of its stages due to changes in the context, the introduction of new external factors, the identification of new needs, the modification of the technological means used, etc., changing the exposure to risk and necessitating a reassessment of risk.

Therefore, the organisation has to implement procedures that detect problems, changes or events in the processing or its environment that are likely to trigger the need to initiate a risk management review cycle. If no problems, changes or events are detected that would trigger the initiation of a review cycle, it will be necessary to establish review periods that could be set in the framework of the data controller's data protection policies[61].

[61] Article 24.2 of the GDPR.

Of vital importance in this process is the management of incidents (of all kinds) or the information that can be inferred from complaints from data subjects in the exercise of their data protection rights.

In particular, in cases where the need for processing may be justified by external events of a temporary or transitory nature, such as emergency situations, sunset clauses should be established in the reassessment of the balance between the interference with rights and freedoms represented by the processing and the social benefit it generates.

It is very important to emphasise, as noted above, that the iteration of a risk management cycle should not be a disproportionate effort, but rather an effective and efficient activity. All it requires is to reflect, if only for a moment, on whether processing remains under control in the face of changing conditions of the processing itself and/or the context in which it takes place.

Moreover, this reflection must be integrated into the processing management processes in order to be truly effective.

IV. GOVERNANCE OF RISKS TO RIGHTS AND FREEDOMS

A. DATA PROTECTION POLICIES

Data governance is the process by which policies and procedures are implemented to ensure effective and efficient management of information in the organisation. These policies are projected into the management of each specific processing. Among the policies that may be necessary in an organisation, data protection policies should at least be considered as a means of risk reduction.

Where personal data is involved, the data governance set up in the organisation must ensure compliance with the rights and freedoms under the GDPR. To this end, the processing of personal data must be supported by the effective implementation of the principles relating to processing (Art. 5 GDPR), taking appropriate measures and providing sufficient safeguards. Under the principle of proactive accountability, policies must be commitments set at the level of the organisation's management.

Recital 78 states *"... the controller must adopt internal policies ..."* and Article 24(2) states *"Where proportionate ... the implementation of... internal policies … data protection policies*[62]". If we understand the term "policies[63]" as the set of guidelines that govern an organisation's actions in a given matter or field, data protection policies define an organisation's approach to the processing of personal data throughout its life cycle.

Therefore, what the GDPR requires in relation to data protection policies is the effective, practical and executive aspect of a set of guidelines, going beyond the reference to the formal aspect of the existence of a document entitled "data protection policy" where the mere formal reproduction of the articles of the GDPR takes place and is reduced to a mere declaration of the controller's willingness to commit to regulatory compliance. In relation to policies, as in risk management, it is important to avoid confusing substance with form, as it is the substance that is required by the GDPR.

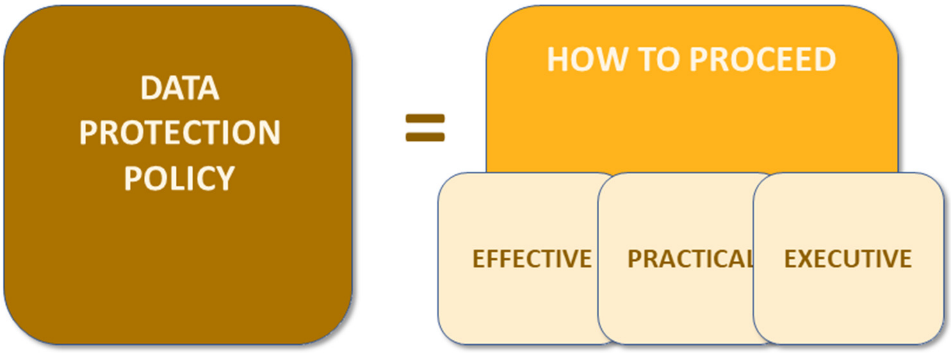


Figure 16: Data Protection Policies

[62] Data Protection Policy should not be confused with Privacy Policy. The latter is a term applied to information clauses that comply with the transparency obligations of the GDPR.

[63] Policy " A set of plans or actions agreed on by a government, political party, business, or other group ".

Of course, in relation to the obligation to demonstrate, such a policy must be documented. However, this requirement does not require the existence of a document with such a title, nor does it require that the policies are defined separately from the rest of the organisation's policies. On the contrary, the practical implementation of the GDPR needs to integrate specific guidelines for better compliance with the GDPR into the documentation of the procedures approved by the entity. Depending on the complexity of the organisation, it is advisable that no new policies or guidelines are created, but that data protection is integrated with existing corporate policies to reduce the administrative and management burden.

In more complex organisations, it may be advisable to have a framework document as long as it is used as a guide for the adoption of the guidelines outlined in specific procedures, e.g. human resources procedures, remote work, procurement of products and services, development of applications, etc. But as long as it is intended to ensure effectiveness in data protection and is not limited to a purely formal statement in a document detached from the reality of the entity's procedures.

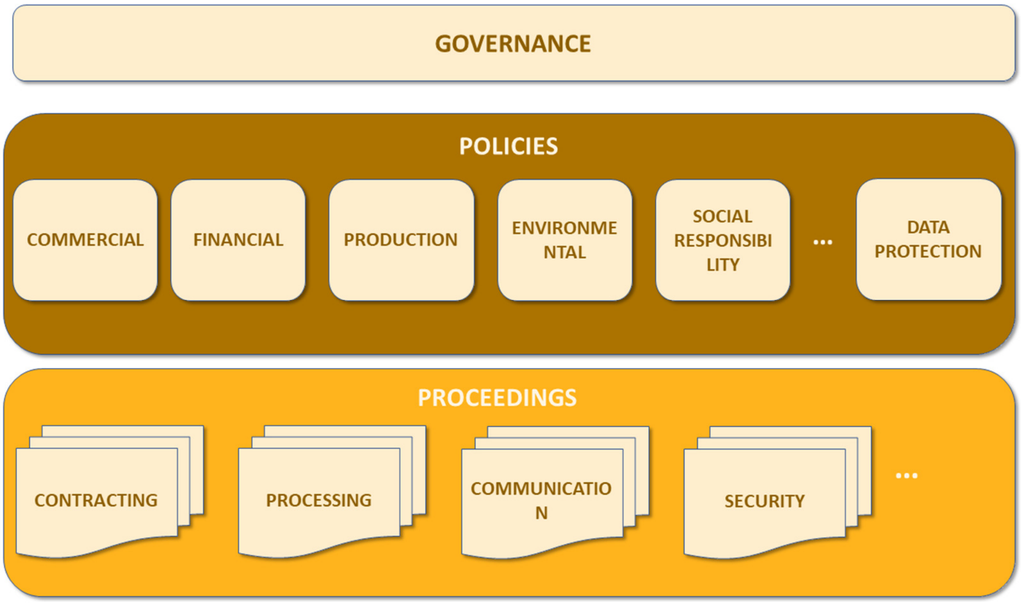


Figure 17: Relationship between Governance, Policies and Procedures

The latter, although an expression of a controller's or processor's commitment to ensure compliance with the GDPR, will be useful as long as it is used as a general guideline when developing the organisation's specific procedures and it is possible to demonstrate that these specific procedures are being used appropriately.

As stated in Article 24, the implementation of such policies and data governance will depend on the organisational structure of each entity. Therefore, the implementation of data protection policies will entail the application of those resources, procedures and controls that may be necessary to ensure such compliance in each specific entity. Similarly, such policies will have to be adopted in organisations that may act as data processors in order to address effective management and control to ensure the controller's compliance with the GDPR.

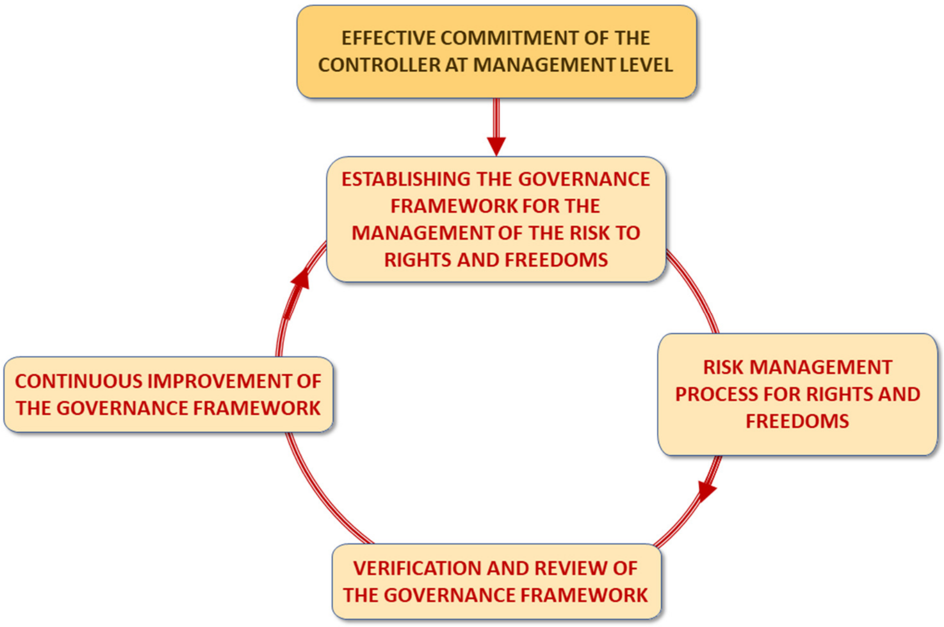

EFFECTIVE COMMITMENT OF THE CONTROLLER AT MANAGEMENT LEVEL
ESTABLISHING THE GOVERNANCE FRAMEWORK FOR THE MANAGEMENT OF THE RISK TO RIGHTS AND FREEDOMS
RISK MANAGEMENT PROCESS FOR RIGHTS AND FREEDOMS
VERIFICATION AND REVIEW OF THE GOVERNANCE FRAMEWORK
CONTINUOUS IMPROVEMENT OF THE GOVERNANCE FRAMEWORK

Figure 18: Data Protection Policy Implementation Framework [64]

Such policies should be verified, reviewed, updated and improved on a continuous basis, in accordance with the criteria and methods implemented in the organisation[65].

B. DOCUMENTATION

The obligation to document the risk management process is related to the fulfilment of the accountability obligation. Documentation has two general objectives:

- Firstly, and most importantly, to support the effective and efficient implementation of risk management for rights and freedoms.
- Secondly, and subordinate to the first, it must be possible to demonstrate that this has been done.

Therefore, the documentation of risk management:

It is a working tool	It should be useful for the effective implementation of risk management.
It must be efficient	It should place a minimal burden on processing management.
It must be complete	It shall record the risk management decisions taken, as well as the justification for these decisions based on objective evidence .
It must be dynamic	It must be maintained and evolve as changes occur in the

[64] Based on ISO-31000 Risk Management - Principles and Guidelines
[65] For example, following a PDCA or continuous improvement cycle.

	processing, in its context or incidences affecting it.
It must be traceable	It will allow the risk management process to be monitored and how it evolve over time.
It must be reportable	It must reach the appropriate decision-making , decision implementation and control bodies.
It has to transmit information	It must have the format, language and content necessary for such actions to be implemented effectively and efficiently
It is not monolithic	It should be made up of different documents, adapted to the different recipients of the information.
It must be integrated into the management of the organisation	In line with what has been stated in relation to data protection policies, it must be integrated with the rest of the documentation associated with the management of data processing in other aspects.

Table 9 Characteristics of Risk Management Documentation

Therefore, documentation is not risk management in the first place, although risk management must be documented.

In turn, documentation does not require writing a single compact document, but having a system for recording analyses, decisions and follow-up actions. The complexity of this system, as interpreted by WP218 Statement[66], should be adapted to the complexity and impact of the processing, and could take different forms, from a spreadsheet to a database or even a document management system.

Risk management documentation is not a legal report either. To the extent that documentation becomes so cumbersome that it does not allow for effective and efficient risk management, it will not be adequate. In this way, all the information necessary for efficient management has to be collected and only this information has to be collected.

[66] 6/ The form of documentation of the processing activities can differ according to the risk posed by the processing. Yet, all data controllers should at least to some extent document their processing activities in order to further transparency and accountability. Documentation is an indispensable internal tool for controllers to manage accountability effectively and for ex-post control by DPAs as well as for the exercise of rights by data subjects. It goes beyond information to be given to the data subjects.

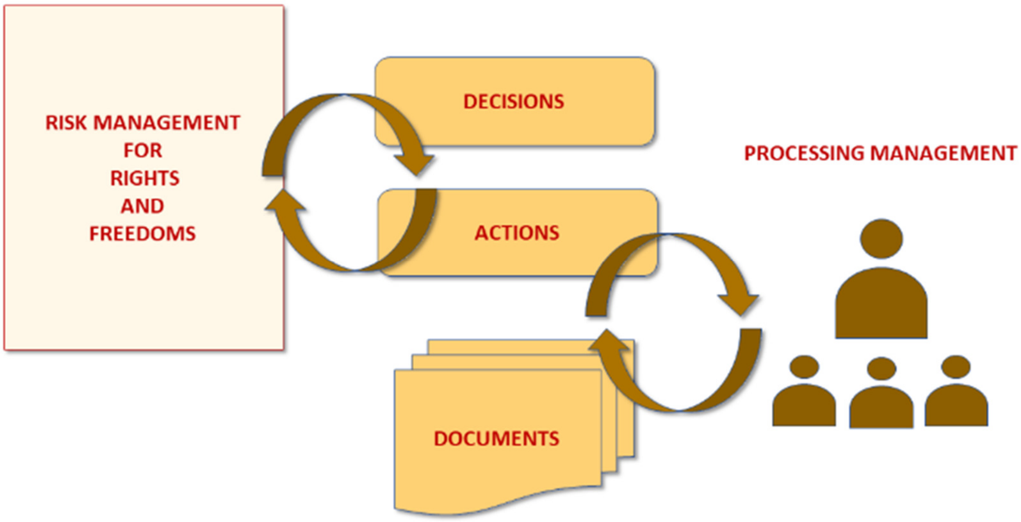


Figure 19: Documentation of the Risk Management Process

The risk management documentation shall contain minimum elements:

1. Who performs it.
2. Who approves it.
3. The description of the processing.
4. Methodologies and guidelines used in the management process.
5. Identifying and analysing risk rights and freedoms.
6. Assessment of level of risk posed to rights and freedoms.
7. The decision whether or not to conduct a DPIA (analysis of obligation and analysis of need for DPIA).
8. The selected measures and an implementation and monitoring plan.
9. Criteria for re-evaluating the plan and timelines for revising the plan
10. Incidents detected
11. Date of completion or revision.

Table 10 Minimum content of Risk Management Documentation

As mentioned above, this information could be a stand-alone document or be integrated into the organisation's processing management documentation. In turn, the description of the processing will have to be congruent with the information recorded in the tools on which the ROPA has been implemented[67].

In addition, with regard to the documentation of the methodologies followed, the following could be documented:

- The decision to choose a particular methodology.
- Identification of the qualitative or quantitative scale used to describe the potential magnitude of the risk.

[67] For example, if the description of the processing fulfils the obligations of the Registry of Processing Activities (ROPA), the same documentation performs the functions thereof. If not, the ROPA should be included in the entity's process management documents.

- Identification of the possible consequences (impact) that a threat may have on the processing and the data subjects themselves if it were to materialise.
- Identification of the likelihood of a hazard materialising, taking into account its vulnerabilities. In general, the greater the number of vulnerabilities, the greater the likelihood of a threat materialising.
- Criteria used for risk assessment and risk level targets considered acceptable.

Regarding the degree of transparency to be applied to the documentation, the WP248 Guidelines stipulate that there is no obligation to publish this information, with the following qualifications:

> *"Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA."*

Therefore, whether or not risk management documentation is disclosed, either in full or in part, may depend on the entity's transparency policies. But it will also have to be assessed whether transparency can help manage risks to rights and freedoms as a privacy by design measure.

Logically, it would not be justifiable or advisable to publish information detailing specific elements of risk management measures that could increase risk. Although risk management cannot be based on the concealment of the measures taken[68], excessive publicity could pose a risk both to the organisation and to the data subjects themselves[69].

[68] What is called “security through obscurity"

[69] The risk analysis may include details of the assets used in the processing: information systems, network topology, product versions used, etc. This information is critical to the organisation and valuable to an attacker seeking unauthorised access to the organisation. This information is critical for the organisation and valuable for an attacker seeking unauthorised access to the organisation, and can be used in combination with other information published by the organisation in different media (social engineering).

SECTION 2: BASIC METHODOLOGY FOR THE IMPLEMENTATION OF RISK MANAGEMENT FOR RIGHTS AND FREEDOMS

V. DESCRIPTION AND CONTEXTUALISATION OF PROCESSING

Proper management of the risk to rights and freedoms requires knowledge of the details of the processing.

The description of a processing is best done in a way that is in line with the description of processes already in use in the entity's management and quality systems. There are only two requirements for such an alert to be adequate. The first is that the description should be extended to include the information set out in Article 30 of the GDPR on the minimum requirements for records of processing activities. Secondly, that the information it contains is sufficient to enable effective risk management for the rights and freedoms of natural persons.

There are different methodologies for formalising a processing study. This chapter provides a methodology for describing processing that is minimal in nature and is intended to assist those who need to implement a methodology from scratch. Any other could be suitable if it complies with the above paragraph. When choosing one methodology or another, it is recommended that it is integrated into the organisation's management systems.

The granularity to be achieved in the description of the processing must be sufficient to enable such management to be carried out. In this regard, processing could be studied at up to three levels of detail:

- High-level processing study.
- Analysis of the structure of the processing, or decomposition of the processing into phases in order to carry out individual phase studies.
- Analysis of Data Lifecycle.

The depth of the processing study, i.e. the decision whether to perform only the high-level study or to go as far as a full data lifecycle analysis, will depend on the possible level of risk and the complexity of the processing.

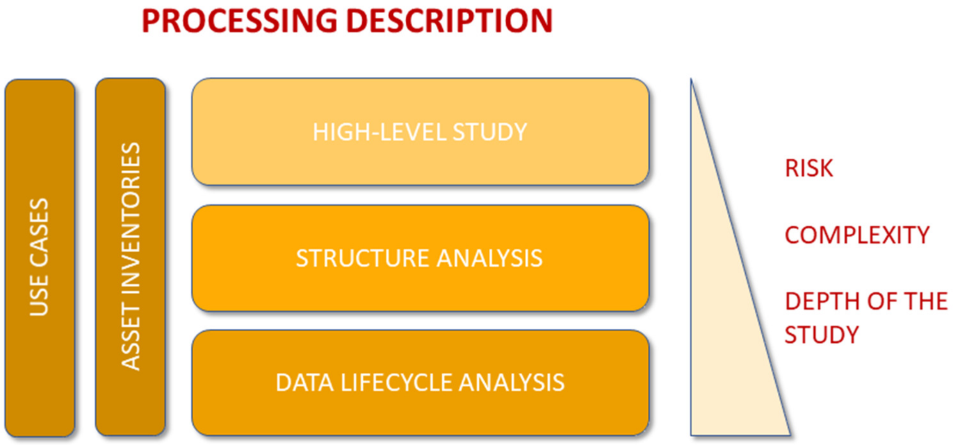


Figure 20: Levels in the Description of the Processing

The information provided by the above levels of description could be completed by additional analyses, such as asset inventory and use case description. All these levels of description are developed throughout this chapter.

Where the controller, with the advice of the DPO if appointed, has doubts about the depth of the study that should be carried out, it is recommended to carry out the structured analysis, as a minimum.

In any case, any approach to the description of processing must aim at having a useful tool to "ensure and be able to demonstrate "[70]efficiently the management of the risk to rights and freedoms. In no case should it become or be interpreted as a mere bureaucratic burden.

A. HIGH-LEVEL PROCESSING STUDY

A high-level processing study approaches processing as a monolithic element, with no divisions or parts. This study should enable a risk analysis to be carried out with the necessary formality, and may also serve to obtain sufficient information to enable compliance with the obligations of art. 30 of the GDPR and 31 of the LOPDGDD (ROPA and inventory).

In the methodology used, such an analysis should be able to provide at least the following information:

Processing	Name or description
Controller/s	Identification of the controller[71].
	Processing purposes
Purpose of the processing	

[70] Article 24 of GDPR

[71] In case of co-responsibility, determine these co-responsibilities and their limits.

Intermediate and secondary purposes[72]	
Scope and field of processing	
Personal data	
Personal data processed	Grouped by category.
Data accuracy	Including, at least: • The frequency of collection. • Granularity.
Life cycle of data	A brief description of its life cycle, including: • Conditions for erasure of data. • Maximum and minimum time the data may be kept for processing.
Data subjects	
Categories of data subjects affected	Establish the possible categories of data subjects for whom the processing is intended to be designed (minors, people at risk of social exclusion, patients, pupils, etc.). It is recommended to analyse possible power imbalances between the data subjects and the controller[73].
Volume of subjects	Number of subjects affected.
Geographical extent	Local, regional, national, or international. Specifying this extent.
Duration of the processing	
Extension of processing time	Both from the start of production to the proposed withdrawal of processing. Description of circumstances that could lead to withdrawal of processing.
Nature	
Implementation of the processing	
Operations executed in processing	Such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Use cases	

[72] Recital 33: It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

[73] WP248 Guidelines

Inventory of assets[74] implementing processing	Specifying: • Human. • Organisational. • Materials. • Technicians/Information systems.
Data collection and generation	
Data source	External to the processing (other processing operations, controllers, or entities) or internal to the processing.
Inferred or generated data	Categories of data inferred in relation to the purposes of processing.
Access to data	
Categories of parties involved in the processing	With regard to the phases of the processing, define the categories of parties involved in the operations.
External parties and their roles	Processors, sub-processors, developers, etc. Phases or stages of processing in which they are involved and the processing operations they are entrusted with by the controller, as well as the legal link with the controller.
Roles of access to the data of the intervening parties	For each party, define their roles in relation to the identified processing operations.
Information flows with other processing operations of the controller	It is necessary to take into account the organisation's processes related to processing (quality management, business intelligence, directories, agendas, etc.) in order to identify the relationship between the processes with the organisation's processing in a single process/processing map.
Data disclosure	Identification of the entities to which data are transferred, with their geographical locations, legal authorisations and safeguards established for such communication, as well as any other information relevant to risk management.
Weaknesses	
Relevant characteristics/constraints and risk factors of the technologies involved	
Vulnerabilities	Derived from technical, but also human or organisational elements, which may lead to unauthorised access or loss of data quality, accuracy, availability, resilience, etc.

[74] Asset is defined as any asset or resource that may be required to implement and maintain a processing activity throughout its life cycle, from conception and design to the end of the processing life.

Measures and safeguards implemented	
Data Protection Policies	
Privacy and security measures and safeguards by default and from the design of the processing	A set of legal, organisational, and technical safeguards incorporated in the processing irrespective of the level of risk that may be associated with the processing.
Privacy and security measures and safeguards adopted according to the risk.	A set of legal, organisational, and technical safeguards that are adopted according to the risk. This section could be empty in the first iteration of the risk management cycle. Depending on whether the risks are being addressed with different measures, this section would be completed.
Safeguards on international transfers	Contractual clauses, BCR's or other.
Context	
Sector of activity	
Market or economic sector	
Regulatory framework	
Regulatory framework for implementation	In addition to data protection regulations, the sectoral regulations applicable to the processing shall be taken into account.
Standards, certification, codes of conduct applicable to the processing	
Possible side/unwanted effects of the processing	
Derived from the scope and field	
Derived from the nature of the data	
Derived from the market or sector	
Other side effects of processing	
Data breaches	
Known incidents in similar processing	Known incidents should be understood as both incidents in the organisation itself and incidents in other organisations with similar or identical technical, organisational, human, etc. means. In this context, it may be helpful to consult the AEPD's security breaches microsite[75].

[75] https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-seguridad

Potential threats	Derived from technical, human or organisational elements, as well as from specific situations or social contexts (economic crisis, pandemic, political or social instability, etc.) which, by exploiting a vulnerability of one of the identified assets, could give rise to breaches with undesired consequences for the rights and freedoms of data subjects:

Table 11 Information derived from a High-Level Processing Analysis

B. STRUCTURED PROCESSING ANALYSIS

In the event that a description of the processing, as shown in the previous section, is not sufficient to manage the risk to rights and freedoms, a structured analysis of the processing will be necessary[76]. To do this, it is necessary to identify in the processing the different operations that make it up and the relationship between them.

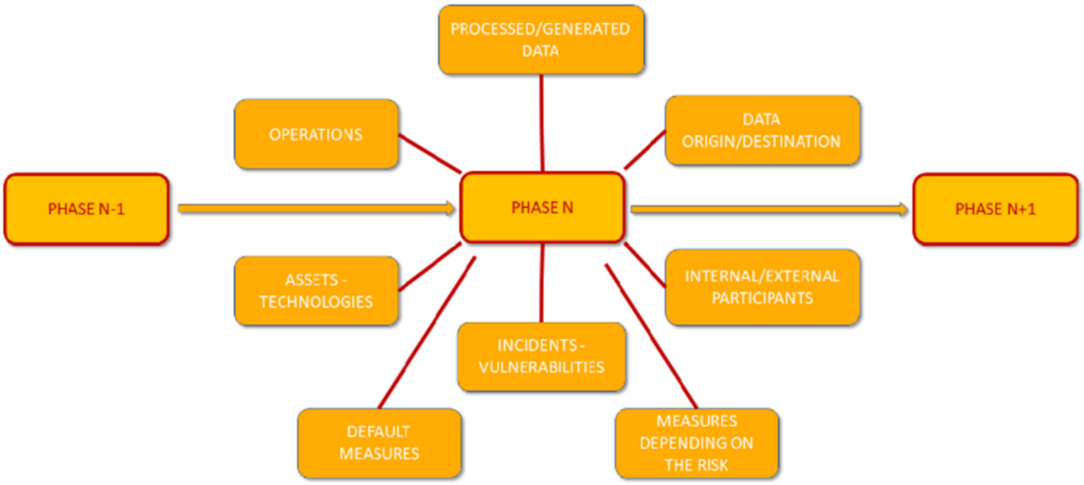


Figure 21: Elements Describing a Processing Phase

The processing operations that may form part of a processing operation and which are of interest for data protection are defined, in a non-exhaustive manner, in Article 4 of the GDPR as:

> *4.2 "processing": ...collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

[76] Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks (WP218): "Data subjects should have the same level of protection, regardless of the size of the organization or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner."

In turn, Article 4 of the GDPR defines two data processing operations that may be incorporated in such processing operations: profiling[77] and pseudonymisation[78].

“Typical" processing will generally include the following phases: data capture, classification, and storage, use and exploitation, transfers of data to third parties, blocking and/or deletion of data.

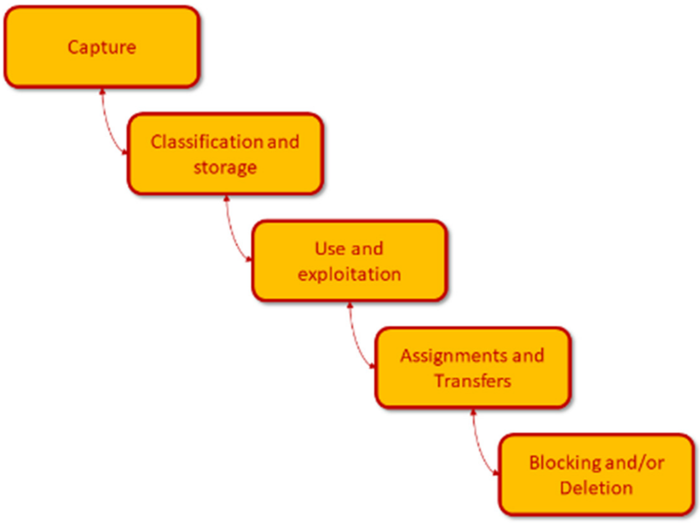


Figure 22: Structuring a generic processing in phases.

This is a simplistic approach but could be a starting point for a structured processing analysis, which could be more complex and include several use cases.

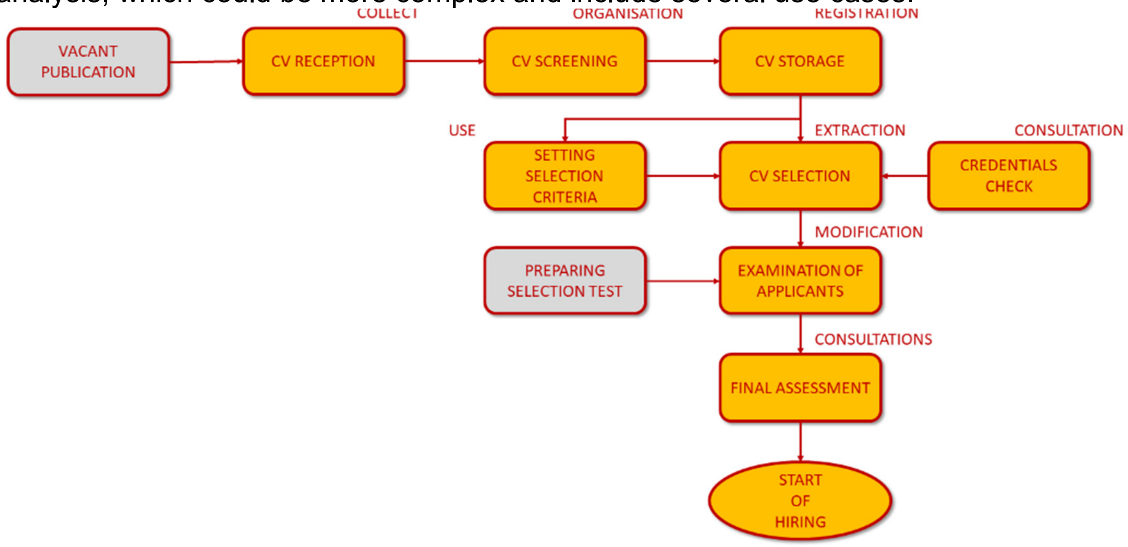


Figure 23: Simplified example of a processing activity relating to personnel selection. In this case, the operation or operations carried out are identified for each phase.

[77] Article 4.4 «profiling»: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;.

[78] Article 4.5 ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Those phases which, in this example, would not process personal data are marked in shading.

The degree of description of each phase would have to be commensurate with the risk impact that the phase could have. As a guideline, in order to manage risk, the following elements could be identified for each phase:

Name of the phase:	
Previous phases	
Subsequent phases	
Operation(s) carried out	Several operations could be executed in the same phase.
Assets implementing the operation	Assets as defined in the previous section.
Relevant features of the implementation phase	Implementation can be done with organisational measures and/or technical elements. Organisational measures may include aspects such as the physical layout of the premises (e.g. isolation of interview areas) or the generation and destruction of physical reports. On the other hand, in the case of technical components, disruptive technologies or novel use of certain techniques, among others, could be identified.
Data processed	
Inferred or generated data	
Data source	External to the processing (other processing, controllers, or entities) or internal to the processing.
Destination of data	External to the processing (other processing operations, controllers, or entities) or internal to the processing.
External actors, their roles, and functions	Processors, sub-processors, developers, etc. and in different functions: editor, support, etc web, administrator, analysis, DB, marketing, etc.
Known incidents of implemented phases with similar characteristics, their own or others	
Vulnerabilities and threats	Derived from technical, but also human or organisational elements, which may result in unauthorised access or loss of

	data quality, accuracy, availability, resilience, etc.
Privacy and security measures and safeguards by default	Set of legal, organisational, and technical safeguards already in place.
Privacy and security measures and safeguards adopted according to the risk	A set of legal, organisational, and technical safeguards that are adopted according to the risk. This section could be empty or have a first approximation in the first iteration of the risk management cycle. Depending on whether the risks are addressed with different measures, this section would be completed.

Table 12 Description of a Processing Phase

C. DESCRIPTION OF THE DATA LIFECYCLE

For complex processing operations, where the main source of risk comes from the sensitivity, the extent of the data, the forms of data collection or their communication to third parties, it is advisable to carry out an overall analysis of the data life cycle. Life cycle analysis involves studying, for a data set or category of data, the different stages of its life, from its collection or generation to its destruction. The description of the data lifecycle is a complementary analysis to the structured analysis of the processing.

Therefore, this study could be limited to one category of data, e.g. biometric data processed in a processing operation, or extended to all categories of data, depending on the exercise of proactive risk management responsibility.

An elementary approach to the study of the data life cycle could be structured in the following stages:

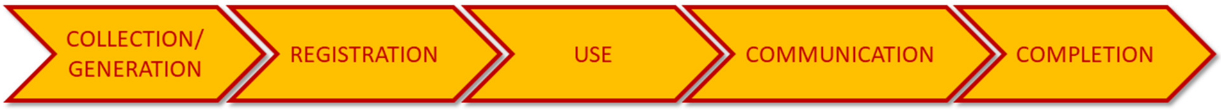


Figure 24: Basic data lifecycle.

- **Collection/Generation:** Process of obtaining data for processing. Data can be collected through a variety of techniques: web or paper forms, sampling and surveys, audio and video recordings, information collected by sensors, etc. But new data can also be generated in processing, such as in profiling, inference of new personal information or automated decision-making.
- **Record:** It consists of establishing categories and assigning them to data for storage, organisation, structuring, preservation or adaptation in systems or files and databases.
- **Use:** It covers the operation or set of operations which is performed upon personal data or sets of personal data, whether by manual or automated procedures, relating to their alteration, retrieval, consultation or use.

- **Communication to a third party:** Includes the transfer or disclosure of data to a third party[79] by transmission, dissemination, or any other form of enabling access, collation or interconnection. It is possible that the communication may, in turn, involve an international transfer of data.
- **Completion:** Limitation processes, including the blocking of data as required by Article 32.2 of the LOPDGDD[80],erasure, or destruction of data.

The following is a possible model for documenting the life cycle of a data category:

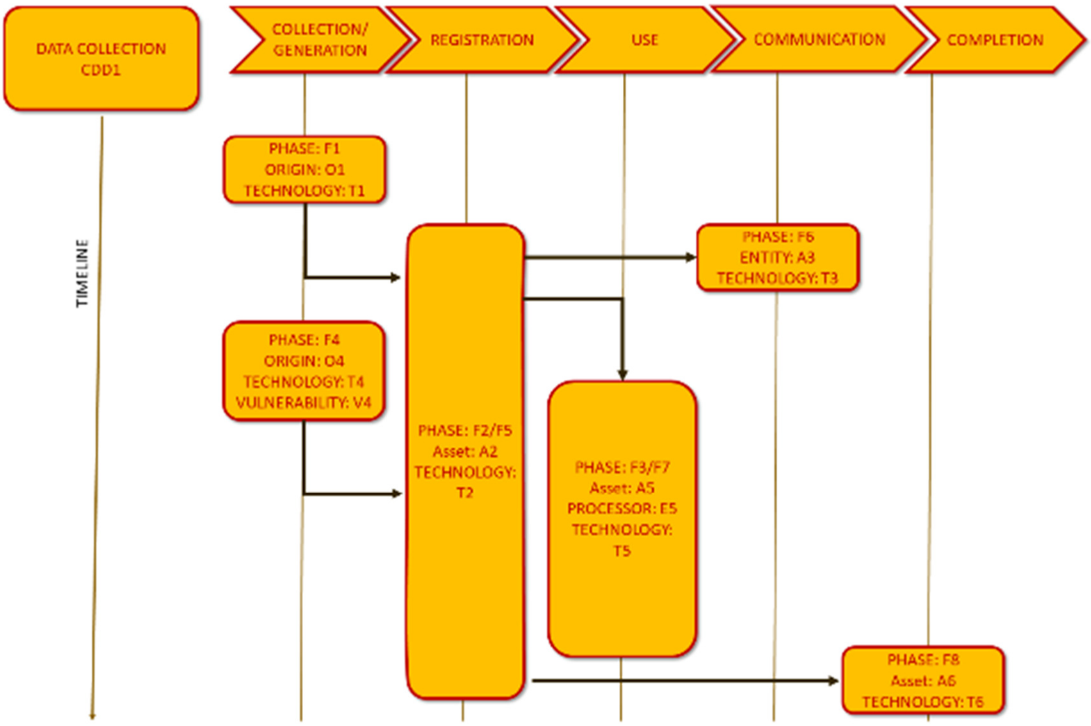


Figure 25: Example of data lifecycle.

In the example shown in the graphic above, additional information has been included, such as reference to the phases involved, processors, third parties, technologies or other information that could be relevant for the description and management of the risk.

[79] Third party (Art.4.10 GDPR) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

[80] Article 32.2 of the LOPDGDD. "*The blocking of data consists of identifying and reserving data, adopting technical and organisational measures, to prevent their processing, including their visualisation, except for making the data available to judges and courts, the Public Prosecutor or the relevant Public Administrations, particularly to the data protection authorities, in order to demand possible responsibilities resulting from the processing and only for the limitation period thereof*".

D. INVENTORY OF ASSETS

Asset is defined as any property or resource that may be required to implement and maintain a processing operation at any stage of its life cycle, from conception and design to decommissioning.

All assets should be included, organised, and kept up to date, in what is called the processing asset inventory. This asset inventory is not only relevant from a data protection point of view, but has application in other basic functions for the management of the entity: accounting, depreciation, maintenance, resource allocation, security, etc. so that its existence is to be expected in those organisations that have implemented quality models. In that case, the management of risks to rights and freedoms will have to be integrated with such an inventory.

In this case, the level of detail to be included in the asset inventory should be such as is necessary to identify and manage risk efficiently and, at the same time, to be able to demonstrate such management.

The asset inventory should be determined on the basis of the structured processing analysis, or by any other procedure determined by the entity to be equally or more effective.

A proper asset inventory at the organisational level, not only limited to processing activities, will allow for the identification of relationships or side effects between different processing. In addition, it can improve the economy of resources needed to carry out such an inventory and the subsequent identification and management of the risks that may arise from each asset.

In an entity it will be common that several processing operations can access the same common datasets and make use of common assets[81] for data collection, processing, communication, etc. These assets that implement common operations and that are shared between different processing operations are, in many cases, inherited systems[82]. In other cases, such as the implementation of applications in mobile systems, the processing operations are developed by means of standard third-party components shared between various applications that make common use of access to data processing services[83].

[81] With organisational implementation, such as a physical customer service desk, as well as technological, such as a web page.

[82] A computer system or application that is still in use due to replacement or redesign costs.

[83] With regard to the potential risks for data protection, consult: Progress of the study by IMDEA NETWORKS and UC3M: "Analysis of Pre-installed Software on Android Devices and its Risks to Users' Privacy" https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-IMDEA-android.pdf

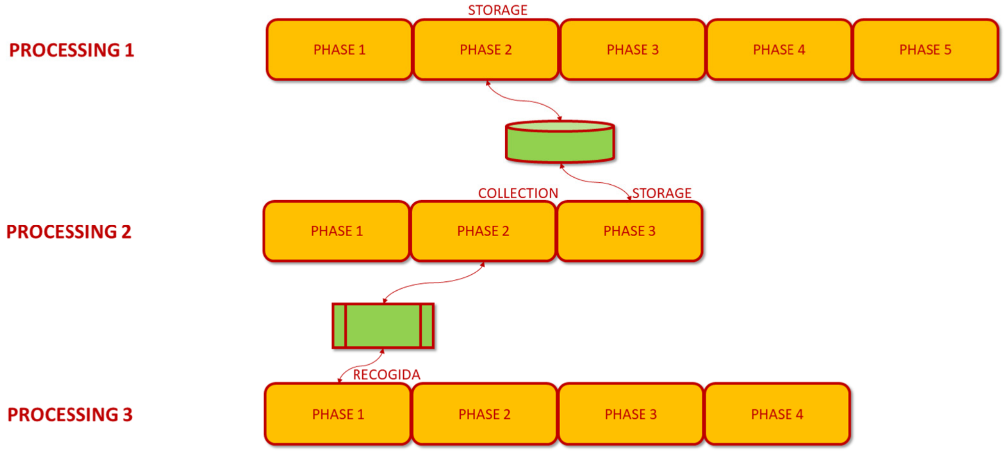


Figure 26: In this case, processing operations 1 and 2 include personal data storage phases, which are implemented in the entity's database services, while processing operations 2 and 3 include data collection phases implemented on the same data capture libraries (for example, an API on Android).

For each asset, it would be possible to document them according to the following model:

Asset:	An asset identifier
Technologies involved:	
Processing and phases in which it is used:	The same asset can be used in different processing
Processing operations where this is necessary:	
Data that are processed:	
Data that are generated:	
Roles with access to the asset and their level of privilege:	
Vulnerabilities (inherent to the asset)	
Threats (internal and external) associated with the asset	

Table 13 Description of assets involved in processing

E. USE CASES

Processing can be very simple, consisting of a simple and orderly sequence of phases. In other, more complex, processing operations, the functionalities, and therefore their characterisation, may vary depending on the configuration of the processing operation, whether set by default or by the user themself, or in relation to the different services that the controller may provide: normal or premium services, suitability for minors, adults or senior citizens, presence of value-added services, etc.

In that case, the description of the processing at the different levels of detail should identify which use case it refers to and mark its differences. The identification of use cases, with examples, has been covered in the Guide to Data Protection by Defect.

VI. IDENTIFICATION AND ANALYSIS OF RISK FACTORS

The identification and analysis of the risk factors for the rights and freedoms of natural persons is the step prior to the assessment of the level of risk of the processing.

This chapter will develop a methodology for such identification and analysis. This methodology is indicative, and is not the only one possible: there is a wide margin of freedom for the entity to choose the most appropriate method according to its characteristics and needs. In particular, it is recommended to use (and extend in relation to data protection) the methodology used for risk management in the organisation.

Similarly, for SMEs and Start-ups in which processing operations are, a priori, low risk, the AEPD provides controllers and data processors with the tools FACILITA-RGPD and FACILITA-EMPRENDE, which, in addition to assisting in regulatory compliance, allow **an initial approach** to risk management. Likewise, the AEPD has published the GESTIONA_EIPD tool, which guides users through the **basic elements** that must be taken into account in the risk analysis of processing operations and in impact assessments. This tool provides the **minimum basis** for initiating risk management activities under the GDPR, including compliance requirements to enable small and medium-sized enterprises, which do not have a risk management framework in place in their organisation, to get started with the identification, assessment, risk management of personal data processing and implementation of DPIA. Finally, there is the prototype of the tool EVALUA_RIESGO GDPR, which aims to help controllers and processors to identify the risk factors for the rights and freedoms of data subjects present in the processing, to make an initial assessment of the intrinsic risk, including the need to carry out a DPIA, and to estimate the residual risk if measures and safeguards are used to mitigate the specific risk factors.

All of the above tools are intended to serve as decision aids and support. These tools generate the basic documentation to initiate risk management, which, as noted above, is a process that guides the effective implementation of measures and safeguards to protect the rights and freedoms of data subjects. However, this result should not be understood as definitive and should be reviewed and adapted to the specific circumstances of the controller in compliance with the obligation of proactive liability imposed on it by the regulation

The only requirement for any methodology used by a data controller or processor is that it is at least as effective as the one presented here for the identification and analysis of risk factors for the rights and freedoms of data subjects.

In the context of active responsibility, the identification and analysis of risk factors shall always be documented and justified so that the controller can demonstrate that the risk management decisions taken at the time were the most appropriate based on the information available ("accountability").

A. IDENTIFICATION OF RISK FACTORS

In the GDPR, and in its development through the LOPDGDD, special regulations, and lists, guidelines and directives approved by data protection authorities, a set of risk factors are identified. These identified factors constitute a list of minimum requirements to be managed.

However, the controller cannot and should not limit themself to addressing the risk factors explicitly identified in the regulations. Risk management must go further, and during the analysis phase, also identify and assess those risk factors that derive from the specific processing according to its nature, scope or extent or the purposes it pursues, without forgetting those that derive from the present context (internal and external to the organisation) and future context of the processing.

B. THE ANALYSIS OF RISK FACTORS

For each of the identified risk factors, the controller shall determine the inherent impact, i.e. the impact that results from not considering measures and safeguards for rights and freedoms. The impact will depend on the harm that may be caused to individual data subjects and to society as a whole, in terms of their rights and freedoms, in the short, medium and long-term.

In turn, it will also be necessary to determine the likelihood of the identified risk materialising.

A priori, in the GDPR we can see two bands or levels of risk defined: high risk to the rights and freedoms of individuals and their absence, which we could call "not high risk". Adjusting the analysis to only the two levels of risk referred to in the GDPR could be a difficulty in establishing effective risk management, as it would limit the granularity for the assessment of residual risk[84] and, in general, for risk management throughout the processing lifecycle.

Under these premises, and as a general approach to achieve a balance between the ease and effectiveness of the risk management process, it is proposed to establish four levels of risk impact (very significant, significant, limited and very limited) as well as four levels of likelihood of occurrence (very high, high, low and unlikely), so that their combined values allow the following risk levels to be established: very high, high, medium and low.

As a proposal, in order to determine the level of a specific risk according to its impact and likelihood, the following heat map can be established:

[84] ISO 31010 recommends as a common approach to divide risks into three bands: intolerable risk, risks where costs and benefits need to be balanced, and negligible risks. It is therefore recommended that the number of risk bands to manage inherent and residual risk should be at least three. However, in order to facilitate integration into the entity's risk analysis processes, one possibility is to implement the same number of risk bands for all areas where the risk management framework applies (environmental, occupational, business, data protection, etc.).

Likelihood	Very high	Medium	High	Very high	Very high
	High	Low	High	Very high	Very high
	Low	Low	Medium	High	Very high
	Unlikely	Low	Low	Medium	Very high
		Very limited	Limited	Significant	Very significant
		Impact			

Table 14 Likelihood x Impact Matrix to determine the Level of Risk

In order to calculate the level of impact, as a guideline and without prejudice to the following chapters, the following considerations could be taken into account:

Level of impact	**Description**	**Fundamental rights**
Very significant	It affects the exercise of fundamental rights and public freedoms established in the Constitution[85],and its consequences are irreversible. and/or The consequences are related to special categories of data or to criminal offences and are irreversible. and/or It causes significant social harm, such as discrimination, and is irreversible and/or It affects particularly vulnerable data subjects, especially children, in an irreversible way. and/or Causes significant and irreversible moral or material losses.	Equality Non-discrimination Life Physical integrity Religious freedom Personal freedom Personal and family privacy Self-image Expression Information Academic Meeting Association Free and equal access to public office and public functions
Significant	The above cases when the effects are reversible. and/or Loss of control of the data subject over their personal data, where the extent of the data is high in relation to the categories of data or the number of subjects.	

[85] The fundamental rights guaranteed by the Spanish Constitution are, among others, the right to equality and non-discrimination; the right to life and physical integrity, religious freedom, personal freedom, personal and family privacy and self-image, freedom of expression and information, academic freedom, freedom of assembly, freedom of association, free access to public positions and functions in conditions of equality, effective judicial protection, criminal law, education, trade union membership and the right to petition.

	and/or Identity theft of data subjects occurs or may occur and/or Significant financial losses to data subjects may occur and/or Loss of confidentiality of data subject to the duty of professional secrecy or breach of the duty of confidentiality and/or There is a social detriment to data subjects or certain groups of data subjects	Effective judicial protection Criminal legality Education Trade union membership Right to petition
Limited	Very limited loss of control of some personal data and to specific data subjects, other than special category or irreversible criminal offences or convictions and/or Negligible and irreversible financial losses and/or Loss of confidentiality of data subject to professional secrecy but not special categories or infringement penalties	
Very limited	In the above case, when all effects are reversible	

Table 15 Criteria for determining the Level of Impact

When there are two or more risk factors pointing to a certain level of impact, we could speak of a cumulative impact coefficient resulting in a higher level of impact than initially estimated.

For the determination of the likelihood, the following criteria could be used.

Likelihood	
Very high	If the risk factor is materialised and not likelihood-dependent, e.g. because the wp248 Guidelines identify the use of a technology as a risk and it is present in the processing. and/or

	Whether there is evidence of several materialisations of this risk in the last year in different entities. and/or Whether there is evidence of such a risk materialising in the last year in the same entity. and/or There are audits/studies that identify important vulnerabilities in organisational procedures or technical means linked to this risk.
High	Whether there is evidence of such a risk materialising in the last year in any entity. and/or Studies show that the likelihood could be high. and/or There are audits/studies that identify possible vulnerabilities in organisational procedures or technical means linked to this risk. and/or The elements linked to the risk factors have been implemented with non-mature technologies or organisational procedures, without following quality standards, without being certified by independent third parties
Low	Whether there is evidence of such a risk materialising in the last 10 years in any entity.
Unlikely	If there is no evidence of such a risk materialising in any case.

Table 16 Criteria for determining the Likelihood of Materialisation of a Risk Factor

In order to correctly assess the above table it is important:

- To justify that the state of the art regarding the elements implementing the processing is known.
- To have access to the vulnerability catalogues of those already existing on the market and that it is duly updated.
- To check incident logs (e.g. the reports published by the AEPD on the micro-site personal data breaches).

When there are two or more indications pointing to a certain likelihood level, we could speak of a cumulative likelihood ratio resulting in a higher likelihood rate than initially estimated.

C. LIST OF RISK FACTORS IDENTIFIED IN THE REGULATION

The GDPR, and the developing regulations, identify multiple risk factors[86]. The person in charge of the risk assessment of a processing should take into account all factors that are already identified and determine whether they affect, or are likely to affect, the processing.

This task requires going through all the legal texts and making an effort to systematise them. To facilitate this, this guide compiles the risk factors identified, groups them into categories, and determines a minimum risk level for each category. In turn, the AEPD has published a prototype tool for assessing the level of risk of a processing operation, EVALÚA_RIESGO RGPD, which allows a first approximation to be made to the identification and assessment of the risk of a processing operation on the basis of the categories shown here.

The categories are as follows:

Operations related to the purposes of processing	Risk factors deriving from the purpose stated of the processing and other purposes related to the main purpose.
Types of data used	Risk factors related to the scope of the processing that arise from data collected, processed or inferred in the processing.
Extent and Scope of Processing	Risk factors related to the scope of the processing relating to the number of data subjects concerned, the diversity of data or aspects processed, the duration in time, the volume of data, the geographical extent, the exhaustiveness on the person, frequency of collection, etc.
Categories of Data Subjects	Risk factors related to the scope of the processing related to the category of data subjects, such as employees, minors, elderly people, persons in a situation of vulnerability, victims, disabled people, etc.

[86] Among them: art.35.3 of the GDPRGDPR, WP248 Guidelines, AEPD list based on art.35.4 of the GDPR, art. 28.2 of the OL 3/2018, art.32.2 of the GDPR, Recital 75 of the GDPR, “Guidelines 8/2020 on the targeting of social media users”, “Guidelines 02/2021 on Virtual Voice Assistants”, “Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications”, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak”; “Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak”, “Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation”, “Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation”, “Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies”, “Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions”, “Guidelines 07/2020 on the concepts of controller and processor in the GDPR”, “Opinion 8/2014 on the on Recent Developments on the Internet of Things”, “Opinion 02/2013 on apps on smart devices”, “Guidelines on Data Protection Officers ('DPOs')”.

Technical Factors of Processing	Risk factors that arise from the nature of the processing when implemented with certain technical characteristics or technologies.
Data collection and generation	Risk factors that arise from the nature of the processing when data are specifically collected or generated.
Side Effects of Processing	Risk factors that arise from the processing context as consequences may occur that are not foreseen in the original intended purposes of the processing.
Category of controller/processor	Context-related risk factors specific to the sector of activity, business model or type of entity.
Data disclosure	Risk factors that arise from the context in which the data disclosures are made to third parties within the framework of the processing
Data breaches	Risk factors that arise from the possible materialisation of personal data breaches.

Table 17 Categories of Risk Factors identified in the GDPR or in its development.

The level of risk, determined for each risk factor in isolation, grouped by category, is as follows:

1. Operations related to the purposes of processing

Risk factors arising from the stated purpose of the processing and other purposes linked to the main purpose.

Risk factor	Level of Risk
Profiling E.g. and without being exhaustive: • Profile creation • Use of profiles • Classification of individuals • Targeting products/services to individuals or groups • Behavioural analysis (assessment and rating of emotions, moods, habits, preferences, etc.) • Other	High

Assessment of subjects e.g. and without being exhaustive: • Valuation • Score • Other	High
Prediction E.g. and without being exhaustive: • Inference of new personal data • Other	High
Employee control E.g. and without being exhaustive: • Employee assessment • Workplace observation • Workplace monitoring • Workplace image recording • Audio recording in the workplace • Image-based monitoring in the workplace • Sound-based monitoring in the workplace • Geolocation of workers en-route • Time spent performing tasks • E-mail monitoring and control • Monitoring and control of Internet browsing at the workplace • Monitoring the use of IT applications/services in the workplace • Telephone usage monitoring • Other	Medium
Internet access control e.g. and without being exhaustive: • Analysis or evaluation of Internet usage times • Analysis or evaluation of Internet browsing activity • Analysis or evaluation of alarms about browsing to specific Internet sites • Analysis or evaluation of navigation alarms to specific content on the Internet • Other	Medium
Observation E.g. and without being exhaustive: • Image surveillance • Sound surveillance • Communications surveillance • Heat or other emissions surveillance • Transmission surveillance • Internet surveillance • Other	High
Monitoring E.g. and without being exhaustive: • IoT-based management • Image-based control	High

• Sound-based control • Communications control • Heat or other emissions control • Transmission control • Internet control • Geolocation-based control • Other	
Supervision E.g. and without being exhaustive: • Control • Image-based analysis • Sound-based analysis • Communications analysis • Heat or other emissions analysis • Transmission analysis • Internet analysis • Geolocation-based analysis • Road traffic control • Other	High
Contact tracing	Very high
Physical access control e.g. and without being exhaustive: • Workplace access control • Access control to commercial premises • Access control to events • Access control to sports facilities • Access control to buildings (public/private) • Other	Low
Location E.g. and without being exhaustive: • Geolocation • Mobility profiling • Determination of usual locations • Identification of frequent access sites • Data about the person inferred from geolocation • Other	Medium
Unique identification	Low
Automated decisions without human intervention	High
Automated processing for decision support E.g. and without being exhaustive: • DSS • Business intelligence that goes beyond purely statistical data • Data mining • Other	Medium
Deciding on or preventing the exercise of fundamental rights E.g. and without being exhaustive: • Right to equality	Very High

• Right to non-discrimination • Right to life and physical integrity • Right to freedom of religion • Right to personal liberty • Right to personal and family privacy • Right to self-image • Right of free speech and information • Right to academic freedom • Right to freedom of meeting • Right of freedom of association • Right to free and equal access to public office and public service • Right to effective judicial protection • Right to criminal legality • Right to education. • Right to trade union membership • Right to petition • Other rights or freedoms	
Decide on the data subject's control of their personal data • Right of access. • Right to rectification • Right to object • Right to erasure • Right to restriction of processing • The right not to be subject to automated decisions without human intervention. • Right to portability • Other	High
Deciding on access to a service	High
Deciding on the execution or performance of a contract	High
Deciding on access to financial services	High
Legal effects on persons	High
Assessment and/or prediction of disease/health potential genetically.	Very High
Preservation for storage purposes	Medium

Table 18 Risk Factors associated with the Operations related to the Purposes of Processing.

2. Types of data used

Risk factors related to the scope of the processing that arise from the data collected, processed or inferred in the processing.

Risk factor	Level of Risk
Personal documents e.g. and without being exhaustive: • Emails • Personal letters • Diaries • Notes on e-readers • Other	Medium
Information from vital activities logger applications	High
Personal aspects E.g. and without being exhaustive: • People or groups with whom they interact • Temperament • Character • Intelligence • Social roles • Adaptability • Risk tolerance • Audio-visual content tastes/preferences (interactive TV, content platforms, social networks, ...) • Health care • Cultural (reading, music, art, ...) • Membership and activities in social and cultural associations • Other	Medium
Consumption preferences, habits, tastes, needs, etc. that do not allow the inference of information related to special categories of data E.g. and without being exhaustive: • Consumption preferences: category of store, type of establishment; type of products; etc. • Consumption habits (customer loyalty cards, web activity, ...) • Preferences for audio-visual content in different media (interactive television, content platforms, social networks, ...) • Leisure preferences (sports, restaurants, museums, theatres, music, etc.) • Other	Medium

Job performance E.g. without being exhaustive: • Workplace access control • Recording images of the workstation • Audio recording at the workplace • Worker assessment by means of images captured from worker devices and displays • Sound-based worker assessment • Image recording in access areas or in offices • Audio recording in access areas or in offices. • Monitoring of employee equipment • Performance inference through indicators (productivity and quality of work, efficiency, training acquired, objectives achieved) • Other	Medium
Economic situation E.g. without beingexhaustive: • Personal income • Monthly income • Assets (movable/immovable) • Employment status • Other	Medium
Financial statement E.g. without being exhaustive: • Financial soundness • Debt capacity • Level of debt (personal loans, mortgages) • Solvency lists • Non-payments • Assets (investment funds, income generated, equities, receivables, income received, etc.) • Liabilities (expenditure on food, housing, education, health, taxes, credit payments, credit cards or personal expenses, etc.; or debts or obligations • Other	Medium
Data on payment methods: E.g. and without being exhaustive: • Credit cards • Information on access to virtual currency services. • Others.	High
Behavioural data E.g. and without being exhaustive: • Reliability of the person • Habits and values that facilitate coexistence • Habits and values that facilitate work and study • Habits and values that influence personal, occupational and family wellbeing • Habits and values influencing engagement with people and society	Medium

• Job stability • Complaints about the person • Other	
Location data E.g. and without being exhaustive: • Register of movement • Location-based register of routines • Register of usual places • Other	Medium
Highly personal data[87] not included in rankings above	High
Health data E.g. and without being exhaustive: • Clinical records • Health reports • Health-related sick leave reports for the Occupational Risk Prevention Service • Prescriptions • Physical health data • Mental health data • Data relating to the provision of health care services • Health data from eHealth applications • Documents relating to the patient's care processes (including identification of doctors and other professionals involved) • Any information that is considered to be significant for accurate and up-to-date knowledge of the patient's health status • Other	Very High
Biometric data E.g. and without being exhaustive: • Fingerprint • Facial features • Iris • Veins in the palm of the hand • Voice • Ear • Gestures	High

[87] Wp248: "Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications

• Gait pattern • Body descriptors of any kind • Other	
Genetic data	Very High
Special categories of data or allowing inferences to be drawn from them e.g. and without being exhaustive: • Ethnic origin • Racial origin • Political opinions • Religious convictions • Philosophical convictions • Trade union membership • Data relating to health • Data relating to sex life • Data relating to sexual orientations • Other	Very High
Special categories of pseudonymised data	High
Personal data relating to convictions and criminal offences	Very High
Metadata E.g. and without being exhaustive: • Electronic communications traffic data • Identification of sender and/or receiver in communications • Data on internet connections: location; software and hardware characteristics of the device with which you are connected; social networks or pages in general to which you are logged in, connection (IP, service provider, download speed), .. • Other	Medium
Unique identifiers E.g. and without being exhaustive: • IP address • MAC address • IMSI • IMEI • Device ID • Telephone No. • NIF, NIE, Passport N. or equivalent • Social Security No. • Vehicle registration number • Credit card number. • UIDs (unique user registration identifiers on websites) • Unique identifiers derived from the characteristics of the device (e.g. access to the battery information of a device, advertising id of the device) • Unique identifiers added to files (e.g. metadata of photographs uploaded to social networks)	Medium

• Other	
Electronic communications data and metadata and inferred electronic communications data E.g. and without being exhaustive: • Emails • Instant messaging • Telephone calls • Video calls • Other	Medium
Web browsing data E.g. and without being exhaustive: • Logging of visited pages (e.g. history of browsing, web server logs, ...) • Logging of the time spent on each page • Logging of the time of the visit to the site • Logging of the number of connections • Logging of mouse activity through the different parts of the website • Browser used • Other	Medium

Table 19 Risk Factors associated with the Types of Data used in the Processing.

3. Extent and Scope of Processing

Risk factors related to the scope of the processing relating to the number of subjects concerned, the diversity of data or aspects processed, the duration in time, the volume of data, the geographical extent, the completeness on the individual, the frequency of collection, etc.

Risk factor	Level of Risk
Systematic E.g. and without being exhaustive: • It is caused according to a system • It is pre-set, organised or methodical • It takes place as part of an overall data collection plan • It is carried out as part of a strategy • Other	High
Exhaustive on persons E.g. and without being exhaustive • A wide range of different elements are collected and dealt with • Multiple spheres of life • Different aspects of personality are covered • Other	High
Involves a large number of subjects e.g. and without being exhaustive: • The number of data subjects concerned is high in absolute numbers	Very High

• The number of data subjects concerned is high in relation to the relevant population • The number of data subjects is relevant in relation to the geographic extent • Other	
The volume of data processed is very high	Very High
The duration of processing is high E.g. and without being exhaustive • The permanence of processing is high • Other	Medium
The processing activity has a wide geographical scope E.g. and without being exhaustive: • Regional, national or supranational level • Other	Medium
Large-scale processing E.g. and without being exhaustive • Processing of data from patients in the regular hospital operations • Processing of the movement data of natural persons using the public transport systems in a city (e.g. monitoring through transport cards) • Processing of real-time geolocation data of customers of an international fast food chain for statistical purposes by a processor specialised in the provision of such services • Processing of data from customers in the regular business of an insurance company or a bank • Processing of personal data for behavioural advertising by a search engine • Processing of data (content, traffic, location) by telephony or Internet service providers • Other	High
Excessive collection of data in relation to the purpose of the processing	High

Table 20 Risk Factors associated with the Extent and Scope of Processing.

4. Categories of Data Subjects

Risk factors related to the scope of the processing related to the category of data subjects, such as employees, minors, elderly people, persons in a situation of vulnerability, victims, disabled people, etc.

Risk factor	Level of Risk
Childs under 14 y.o.	Very High
Victims of gender-based violence	Very High
Children dependent on vulnerable subjects	Very High
Persons under guardianship and custody of victims of gender-based violence	Very High
Elderly people with some degree of disability	High
Elderly people	Medium
People with mental illness	Very High
Disabled	High
Persons who access social services	Medium
People at risk of social exclusion	High
Employees	Low
Asylum seekers	High
Patients	High
Vulnerable subjects E.g. and without being exhaustive: • In a situation of particular vulnerability • There is an imbalance between the position of the data subject and the controller • Other	Very High

Table 21 Risk Factors associated with Data Subject Category.

5. Technical Factors of Processing

Risk factors arising from the nature of the processing when implemented with certain technical features or technologies.

Risk factor	Level of Risk
Hospital information system	High
Interactive TV	Medium
Web services	Medium
Mobile applications	Medium
Location registration systems	High
Facial recognition	High
Fingerprint	High
Internet of Things (IoT)	Very High
Innovative use or new organisational solutions	High
Innovative use of established technologies E.g. and without being exhaustive: • Technologies where no assessment has been made of the impact on privacy • Technologies used on a new scale • Other	High
Technologies combined with other technologies	Medium

New technologies E.g. and without being exhaustive: • Immature technologies • Emerging technologies • Other	High
High degree of fragmentation of the actors involved in the development and implementation of the products/services implementing processing	High
Automated processing e.g. and not exhaustive: • processing carried out by an automatic process without human intervention • Other	Medium
Intelligent System	Medium
Video surveillance	High

Table 22 Risk Factors associated with Technical Processing Factors.

6. Data collection and generation

Risk factors arising from the nature of the processing when data are collected or generated in a specific way.

Risk factor	**Level of Risk**
Access to credit reference database	Medium
Access to fraud database	Medium
Access to money laundering/terrorist financing database	High
Personal data obtained in publicly accessible areas e.g. and without being exhaustive: • Motorway • Shopping centre • Street • Station • Market • Library • Other	Medium
Collection of data from public social media	Low
Collection of data from communications networks.	Medium
Collection of data from applications	Medium
Data from two or more processing operations for different purposes	Medium
Data from two or more different controllers	Medium
Association of datasets	Medium
Combination of datasets E.g., and without being exhaustive: • Cross-referencing of databases • Sensor data fusion • Other	High

Linking of database records of two or more processing operations for different purposes or by different controllers	Medium
Collection of data by a controller other than the one processing and applying information exception 14.5 (b, c, d)	Medium
Lack of transparency of the precise timing of data collection. E.g. and without being exhaustive: • Mobile systems • IoT • Domestic assistants • Connected cars • Others.	High
New forms of data collection with risks for rights and freedoms	High

Table 23 Risk Factors associated with Data Collection and Generation.

7. Side Effects of Processing

Risk factors that arise from the context of the processing because of the potential for consequences not contemplated in the original intended purposes of the processing.

In this case, the AEPD has not assessed the level of risk, but only the impact it could have. The controller will have to assess the likelihood of these threats materialising in their processing, therefore the column "Likelihood" is left empty. Once completed, the level of risk can be determined using, for example, the "likelihood x impact" risk matrix shown at the beginning of this chapter.

Risk Factor	Impact	Likelihood
Exceeds the data subject's expectations e.g. and without being exhaustive: • Excessive exposure of the data subject • Segmentation that exceeds reasonable expectations • Inference of interest or other characteristics based on non-obvious data and resulting in a profiling of the subject • Other	Medium	
Possible unauthorised reversal of pseudonymisation	Very High	
Possible loss of control by the controller over the data processed by the processor.	High	

It could determine the financial situation	Medium	
It could determine the capital solvency	Medium	
It could deduce information related to special categories of data	High	
May deprive data subjects of their rights and freedoms	Very High	
May prevent control over their personal data	Very High	
May lead to exclusion	High	
May lead to discrimination	Very High	
Possible identity theft	Very High	
Possible fraud	Very High	
Possible reputational damage	Very High	
Possible Significant Economic Injury	Very High	
Possible significant moral harm	Very High	
Potential for significant social harm	Very High	
Possible loss of confidentiality of data subject to professional secrecy	Very High	
May prevent the exercise of a right	High	
May prevent access to a service	High	
May prevent access to a contract	High	
It may collect personal data other than from service users. E.g. and without being exhaustive: • Home IoT • Smart speakers • Connected cars • Other	High	
Possible manipulation of persons E.g. and without being exhaustive: • Influencing behaviour and decisions of individuals. • Undermine their autonomy and individual freedom. • Generate disinformation. • Focalisation affecting access to pluralistic information • Filter bubble • Information overload • Other	High	
Possibility of self-censorship	High	
Possibility of bringing about a cultural change to surrender rights and freedoms	High	
Unforeseen or unintended uses that could affect fundamental rights.	High	

Table 24 Risk Factors associated with Processing Side Effects.

8. Category of controller/processor

Risk factors arising from the specific context of the sector of activity, business model or type of entity.

In this case, generally understood for processing that are not part of the entity's support[88] processes:

Risk	Level of Risk
Information company	Medium
Biotechnology company	High
Marketing company	Medium
Hospitals	High
Private researchers	Medium
Credit reporting institution	Medium
Fraud assessment institution	Medium
Financial institution	Medium
Employer	Low
Research projects	Low
Clinical test	High

Table 25 Risk Factors associated with Category of Controller/Processor.

9. Data disclosure

Other risk factors identified in the processing that are not specifically identified in the GDPR or its implementation.

Risk factor	Level of Risk
Regular transfer to states or organisations in other countries without an adequate level of protection	Very High
Lack of transparency of the actors involved in the processing process E.g. and without being exhaustive: • Some types of social networks, • Types of digital marketing networks, • Types of blockchain-based processing, • Types of remote continuous learning AI. • Other	Mediu m

[88] Support processes are those that support the entity's business, key or strategic processes. The "customers" of these processes are internal, such as payroll, quality control, personnel selection, personnel training, purchasing, information systems, etc.

Free dissemination of unique identifiers. E.g. and without being exhaustive: • RFID Tags • SSIDs • MACs • Public keys • Others.	High

Table 26 Risk Factors associated with Data Disclosure.

D. RISK FROM PERSONAL DATA BREACHES

In practice, the risk level assessment process cannot be carried out without taking into account the possible consequences of personal data breaches on data subjects in order to establish criteria for consistency in the risk assessment by preventing that the initial risk assessment may differ in relation to the consequences on data subjects resulting from loss of confidentiality, integrity, availability of data, reversal of anonymisation/pseudonymisation, use of data for non-compliant purposes, breach of guarantees, etc.

In the identification and analysis of risk factors, it is necessary to determine the potential harms of the materialisation of personal data breaches in their different dimensions. In this case, both breaches and the notion of security have to be understood in an extensive way, including problems that may occur on the technical risk mitigation measures themselves (e.g. pseudonymisation measures), as well as technical problems in data processing systems (e.g. in transactional systems).

1. Basic Analysis

A basic approach to determining the level of risk is to consider the high-level processing, without going into the detail of the assets that implement the information processing and, from there, to assess the impact that a personal data breach would have on each of the following dimensions: confidentiality, integrity, availability, authentication, traceability, resilience, failures in privacy safeguards and errors in the technical operations[89] of the processing (or C,I,A,AU,T,R,F,E).

To conduct the analysis, the different scenarios of a personal data breach, as defined in Chapter III of this guide, can be considered in order to determine what impacts on data subjects might occur. For each scenario, the following table could be completed:

[89] For example, such as errors in biometric recognition systems, in inferences in AI, in the exchange of data in transactional systems, in the separation of virtual machines etc.,

Processing	Scenario N
Data breach materialised	Description of the type of breach.
Compromised data	List of data compromised in the breach.
Damage to the data subject	Detail what damage could be caused to the rights and freedoms of the data subject and, in general, to their interests. Also defining the extent in data subjects.

Table 27 Description of a Personal Data Breach Scenario.

Based on the harm caused to data subjects, it is possible to determine the impact using the same approach as in the section "Risk analysis" in this chapter. For example, if we estimate that a confidentiality breach irreversibly affects constitutional rights, we would determine that the impact is maximal.

Size of the breach	Impact on Rights and Freedoms
Confidentiality	Maximum / High / Medium / Low
Integrity	Maximum / High / Medium / Low
Availability	Maximum / High / Medium / Low
Traceability	Maximum / High / Medium / Low
Authenticity/Identity	Maximum / High / Medium / Low
Resilience	Maximum / High / Medium / Low
Data breaches in measures and in technical and organizational safeguards of data protection	Maximum / High / Medium / Low
Errors in technical data processing operations	Maximum / High / Medium / Low

Table 28 Compilation of Impact Level for cases of Personal Data Breaches.

In turn, it is necessary to determine the likelihood of these data breaches materialising, for which the table used in the section "The risk analysis" could be used to obtain the following result for each dimension:

Size of the data breach	Likelihood of materialisation
Confidentiality	Maximum / High / Medium / Unlikely
Integrity	Maximum / High / Medium / Unlikely
Availability	Maximum / High / Medium / Unlikely

Traceability	Maximum / High / Medium / Unlikely
Authenticity/Identity	Maximum / High / Medium / Unlikely
Resilience	Maximum / High / Medium / Unlikely
Breaches in measures and in technical and organizational safeguards of data protection	Maximum / High / Medium / Unlikely
Errors in data processing operations	Maximum / High / Medium / Unlikely

Table 29 Compilation of Likelihood of Personal Data Breaches Materialising.

The likelihood analysis will need to consider whether the processing is expected to be operational in the short, medium or long term, as it is important to be aware, as noted above[90], that the likelihood of materialisation will increase over time. For example:

Likelihood Today	**Evolution of Likelihood**		
Maximum	Maximum	Maximum	Maximum
High	High	Maximum	Maximum
Medium	Medium	High	Maximum
Low	Low	Medium	High
	Short-Term < 1 year	Medium-Term < 5 years	Long-Term Longer than 5 years

Table 30 Evolution of the Likelihood of a data breach materialising over time

The level of risk for each dimension of the data breach would be assessed with the following table:

[90] In the section on personal data breaches in Chapter III on the risk management process.

Dimension: C/A/I/T/AU/R/F/E					
Likelihood	Very high	Medium	High	Very high	Very high
	High	Low	High	Very high	Very high
	Low	Low	Medium	High	Very high
	Unlikely	Low	Low	Medium	Very high
		Very limited	Limited	Significant	Very significant
		Impact			

Table 31 Likelihood x Impact Matrix to determine the Level of Risk of a Personal Data Breach

2. Processing of Large Datasets

For processing large volumes of data, it will be necessary to analyse the impact and likelihood of threats materialising on different datasets in different ways:

- On a small dataset, or even on a single individual.
- On a massive volume, or even the total set, of processing data.

A priori, it might seem that a breach affecting a large extent of data and data subjects is less likely than a breach affecting little data or few data subjects.

Small Breach	< Impact	> Likelihood
Large Breach	> Impact	< Likelihood

Table 32 Possible Relationship between Impact and Likelihood on data breaches subject to the Volume of Data.

However, such a presumption should be confirmed by evidence-based analysis. And, even if this were the case, it would have to be determined whether the variations are of the same order of magnitude, so that an increase in the impact would be offset by the same degree of decrease in the likelihood of the breach materialising.

In either case, it is necessary to examine processing considering both possibilities to determine worst-case risk levels.

3. Analysis of the Assets identified in the Processing

In more complex processing, a more detailed analysis could be undertaken by looking at each of the assets identified in the processing in relation to the different dimensions of the breaches.

For this purpose, a table would be made for each dimension. Each table would include the set of assets identified in the processing description. From there, it would be determined, for each asset, whether a breach in the asset dimension is likely to occurif so, the likelihood of its occurrence would be estimated.

Dimension:	C/A/I/T/AU/R/F/E	
Assets	**Likelihood**	**Impact**
Active 1	Likelihood of materialisatio n	Level of impact in terms of how a total or partial loss of the asset in dimension C/A/I/T/AU/R/F/E could affect the rights and freedoms of data subjects.
…	…	…
Asset N	…	…

Table 33 Analysis of the Assets involved in the Processing.

The level of risk for each dimension could be determined by the worst case of the pairs (Impact, Likelihood). In addition, this type of analysis would make it possible to identify the assets on which to make the greatest effort in implementing measures and guarantees to reduce that level of risk.

E. RISK ACTORS NOT EXPLICIT IN THE REGULATION

The risk factors identified in section "C" of this chapter are exclusively those explicitly identified in the GDPR and its implementation. As noted above, it is necessary to study the peculiarities of the processing in order to identify risk factors for additional rights and freedoms. In the interest of applying proactive liability, the controller must carry out a critical analysis of its processing in order to identify those unique situations that could pose a risk factor.

The following is a list of other possible risk factors, not intended to be exhaustive, but as an example that other factors may exist in specific processing. The purpose of this list is to serve as an aid to reflection for those controllers and processors:

Risk factor	Impact	Likelihood
Internal context of the organisation		
Lack of maturity in the organisation's governance and processes		
Internal organisational crisis		

Existence of other high-risk processing in the organisation		
Acting as a processor for numerous (hundreds or thousands) of controllers		
Other		
Operations related to the purposes		
There is frequent and repeated contact with data subjects in a manner that may be intrusive to the privacy of the data subject		
There is a real likelihood that the data will be processed in the future for purposes other than those envisaged at the time of collection, in particular if these purposes are more intrusive or exceed the expectations of the data subjects		
Moulding or presentation of the digital reality based on a profile		
Nudging or positive reinforcement to influence behaviour by exploiting cognitive biases or psychological weaknesses		
Other		
Extent and Scope of Processing		
processing involves a large number of actors and/or organisations and may represent a risk of loss of control of the personal data		
Other		
Technical Factors of Processing		
Educational platforms		
Internet of Bodies/Wearables		
Neurological interfaces		
Artificial Intelligence		
Blockchain		
Other		
Category of controller/processor[91]		
Public bodies and public administrations		
Teaching and education centres		
Insurance company		

[91] In relation, generally, to non-supporting processes.

Other		
Data collection and generation		
False positive rates		
False negative rates		
Other		
Side effects		
Possible inference of special categories of data from the accumulated information from the user		
Affects or is likely to affect the best interests of the minor		
Discrimination in the offer of options, products or services due to user profiling		
Limitation of the freedom of autonomy		
Decision-making biases		
Algorithmic discrimination		
Cultural aspects affecting perception of intrusion or interpretation of data		
Other		
Data disclosure		
Timely transfer to states or organisations in other countries without an adequate level of protection		
Other		
Those foreseen in the codes of conduct to which the entity adheres		
Foreseen in the certification schemes		
Any other risk factor		

Table 34 Examples of other Possible Risk Factors

F. HIGH-IMPACT ANALYSIS

A high-impact analysis should be carried out in special cases: for the case of processing where the commitment to the basic guarantees of the rule of law could be affected and have a very high impact on the rights and freedoms of citizens at the societal level.

In general, we would be talking about cases where there is massive processing of population data. Some processing with such characteristics could be found e.g. in:

- The Public Authorities.
- Telecommunications entities.
- Financial institutions.
- Insurance companies.
- Large health service systems.
- Internet or Cloud service providers.
- Others of equal relevance.

Under these assumptions, and only for these very high impact cases, it would be necessary to assess the relative risk associated with the materialisation of the following events:

Risk factor	Level of Risk
Breakdown of the rule of law	
Radical alteration of legal safeguards	
Geostrategic changes	
Disruptive technological advances	
National emergencies	
Other	

Table 35 Examples of High-Impact Cases

Of course, the likelihood of these events materialising is expected to be minimal, but it can never be considered zero or impossible, so it is important to keep in mind that the level of risk for such situations also needs to be determined.

VII. ASSESSMENT OF THE LEVEL OF RISK RELATED TO THE PROCESSING

The assessment of the total risk level of the processing is derived from the result of the risk level assessment for each of the risk factors identified in the processing. The interdependence of the different risk factors could raise the level of processing risk above the worst case of each risk factor taken individually.

In the event that the processing does not fall within the cases listed for which a DPIA is required (see chapter "Analysis of the obligation to conduct a DPIA), it is necessary to assess the level of risk of the processing. The objective is both to determine whether or not it is mandatory/necessary to carry out a DPIA and to determine the specific level of risk of the processing in order to implement the appropriate measures and safeguards.

When there are different risk factors, it is necessary to interpret how these factors, considered independently, might interact with each other to increase the level of processing risk (cumulative risk factor), by analysing their combined dependencies and effects or the mutual interactions that exist between them.

Given a set of identified risk factors for processing, and their associated level of risk, different methodologies can be used to assess the total level of risk resulting from processing. As regards the specific methodology for determining the level of risk of processing to the rights and freedoms of individuals, it is recommended that it be integrated into the organisation's general methodology.

By definition, in any methodology, the risk level of the processing shall not be lower than the level of the highest value risk achieved by an identified risk factor in that processing individually.

A. SIMPLIFIED APPROACH

A simplified approach to determine the level of risk in a generic way is to establish a simple formula for assessing the accumulation of risk factors as follows:

- The value of the level, for each identified risk, is quantified as follows:
    - Low: 0.2
    - Medium: 0.5
    - High: 0.7
    - Very High: 0.9
- If for a set of identified risk factors {RF1, RF2, RF3... RFn} the following risk levels {RL1, RL2, RL3... RLn} have been assessed, the processing risk level PRL of the processing could be calculated as:
    - PRLa = (RL1 + RL2) – (RL1 * RL2)
    - PRLb = (PRLa+ RL3) – (PRLa * RL3)
    - …
    - PRL = (PRLn + RLn) – (PRLn * RLn)

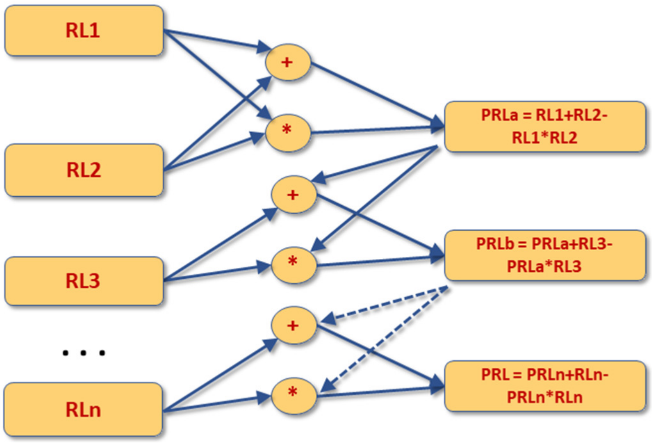


Figure 27: A Simplified Way of Calculating Risk related to the Processing.

- The final result could be interpreted as follows:
  - Low risk related to the processing: if it is less than 0.4
  - Medium risk related to the processing: 0.4 to less than 0.6
  - High risk related to the processing: 0.6 to less than 0.9
  - Very High risk related to the processing: greater than or equal to 0.9

B. DEPENDENCY ANALYSIS APPROACH

Risk factors are not watertight, isolated compartments. Risk factors may have relationships with each other, both with other risk factors within the processing and with other processing being implemented in the same entity, having additive, multiplicative or even exponential effects.

The analysis of such dependencies is used in the security risk analysis in relation to assets[92] and is restricted to this field, although it can be extended to all risk factors in data protection.

In this case, assets are often shared resources between several processing or processes of the organisation, so we could speak of the risk factor as the risk inherited by some assets from those assets on which they depend, in particular the result of accumulating the risk inherited between assets in terms of likelihood and impact. In this regard, it will be necessary, where appropriate, to carry out an asset dependency analysis and to allocate the value of the risk passed on to the higher-level asset based on the risks of the lower-level assets on which it depends.

[92] https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.8/web/help/html/magerit_risk_deflected.html

VIII. CONTROLS TO REDUCE RISK

Once the risk factors have been identified and the level of risk of processing has been determined, the level of risk shall be reduced to an acceptable value.

The following is a list of measures and safeguards, generically referred to as controls, that could be adopted to manage the risk to data subjects' rights and freedoms in the following dimensions:

- The processing concept
- The data protection governance and policies
- Data protection by design
- Security in processing

This list is not intended to be exhaustive, but illustrative of possible measures that exist to address the risks. Nor is it a mandatory list of minimum measures to be taken in any processing. The controller or processor has to manage the risk by addressing the specific peculiarities of its processing. In this regard, the controller or processor must select or define the most appropriate measures and safeguards to address the specific risks that have been identified.

A. MEASURES ON PROCESSING CONCEPT AND DESIGN

These measures will act on the very definition of the nature, scope, context or purposes of the processing, i.e. the essence of the processing as it is conceived and designed. Possible measures or safeguards that could be taken include:

As for nature:	
	Change, rearrange or reorganise the phases of processing.
	Eliminate some phase of processing.
	Isolate and segregate processing steps from each other so that they process data in a more limited way. For example, by ensuring that some steps do not process personal data (e.g. anonymised data) or by using their pseudonymisation.
	Review data processing procedures.
	Change technical choices to implement processing operations by less invasive and/or more mature technologies.
	Switch, in the above sense, to technologies that are more reliable from a data protection point of view, by using for example, the use of PETs (Privacy Enhanced Technologies).
	Replace automated processing with manual processing incorporating monitoring and control procedures.
	Carrying out human supervision of automated decisions .
	Use specially qualified personnel at certain stages of processing, especially in their supervision.

	Redesign the procedures for collecting, enriching or generating personal data.
	Reorganise the physical spaces where processing is carried out.
	Redesign the orientation of work towards local, online or teleworking.
	Check the possibility of implementing alternative means of processing: automatic/manual, different automation options,…
	Limit access to personal data that is required to be held in the system under the management of processors.
	Others.
As for scope:	
	Target processing to a smaller number of subjects.
	Focus processing on covering fewer areas of the subject's life.
	Target processing to a limited geographical area.
	Limit the number of interveners or participants.
	Limit, in the design of the processing, the amount of time which the processing uses data of the same subjects.
	Limit the degree to which the processing interacts or is linked to other processing of the same entity.
	Limiting the extension of processing to subjects considered vulnerable (the elderly, child, handicapped, etc.)
	Define, within the processing, concrete use cases with disjoint scopes.
	Others.
As for context:	
	Define the social or economic contexts in which the processing will be applied.
	Define restrictive use cases targeted at specific sectors.
	Select processors to minimise legal, social or political risks.
	Limit links or relationships with other controllers' processing[93].
	Others.
As for purposes:	
	Limit or redefine the purposes of processing.
	Eliminate secondary purposes in processing.
	Define, within the processing, specific use cases for independent purposes.
	Others.

Table 36 Examples of Possible Measures on the Processing Concept

B. GOVERNANCE MEASURES AND DATA PROTECTION POLICIES

There are a number of measures and safeguards that could be implemented when deploying data protection policies as part of the governance of the processing. These controls straddle the line between specific measures designed for processing and measures put in place as part of the governance of the organisation.

[93] For example, when customer tracking processes in shopping centres are supported by the same service that supports different managers with a technology that allows linking the activity of the same person.

As for the governance framework:	
	There is a specific mandate and commitment from the organisation's management regarding the management of risk to the rights and freedoms of the data subjects.
	Risk management for the rights and freedoms of data subjects is integrated into the organisation's management processes.
	There is an explicit reference to the risk management policy for rights and freedoms in the organisation's risk management framework.
	Measures implementing risk management policies for rights and freedoms are differentiated from policies for managing compliance risk, legal risk or civil and criminal liability risk.
	The roles and allocation of responsibilities and resources necessary to ensure data protection in the organisation are defined.
	The necessary resources are in place to ensure data protection in the organisation.
	The cycle of continuous improvement is in place to ensure that data protection policies are effective and appropriate to the nature, context, scope and purposes of the various processing operations throughout its life cycle.
	There are tangible indicators on the effective implementation of data protection policies.
As for data protection advice:	
	The DPO has been appointed or the collegiate body has been defined;this will exercise the functions of the DPO in the organisation (Articles 37, 38 and 39 GDPR) even though it is not mandatory[95].
	The involvement of the DPO in the procedures for deciding and defining processing operations is established.
	Internal channels for communication with the DPO are defined, as well as the data protection advice and/or those responsible for managing risks to rights and freedoms.
	Actions have been implemented so that the members of the organisation are aware of the role of the DPO, the data protection advisor and/or the person responsible for the management of risks to the rights and freedoms of their functions and the channels for communicating with them.
	The advisory and supervisory duties (Art. 39.1.a and b) of the DPO or the data protection advisor extend to the development, maintenance and surpervision of data protection policies.
	Others.

[94] For example, if the organisation has adopted ISO 31000, with the implementation measures of the risk management framework.

[95] Where the appointment of a DPO is mandatory, this appointment is not subject to the outcome or need arising from risk management.

As for data protection policies embedded in procedures:	
	Active accountability strategies for data protection are included in the procedures for the conception, design and implementation of new processing operations: risk management for rights and freedoms, data protection by design, data protection by default, transparency of processing and security by design, and by default.
	Included in the procurement procedures for products, systems or services that are to implement operations within the processing activity are the requirement for information and guarantees[96] to ensure and be able to demonstrate that such processing complies with the GDPR.
	The points of contact within the organisation for each processing of personal data are designated.
	The complaint boxes implement the management of abuses in the areas of data protection.
	Data protection is integrated into the working procedures at local, remote and teleworking.
	There is a BYOD policy that integrates data protection requirements.
	The processing management policy includes the conditions for the verification and processing of risk management for rights and freedoms.
	Expiry clauses in the processing conditions are set out in the processing management policy.
	Others.
As for the attention to data subjects[97]	
	To the extent that they can result in a decrease in risk, provide procedures for addressing entitlements that go beyond the minimums set out in Chapter III of the GDPR.
	To the extent that they can result in a decrease in risk, have transparency policies that go beyond the minimums set outin Chapter III of the GDPR[98].
	To have channels of communication with data subjects in relation to the privacy protection.
	There are procedures for consultation with data subjects regarding the protection of their rights.
	Other

[96] These can be of various types: independent audits, certifications or others; whether at technical, compliance, procedural or other levels.

[97] Remember that data subjects are not only customers, but also stakeholders, to the extent that their personal data are processed, employees, other natural persons with whom the entity has a relationship and any other person indirectly affected by the processing.

[98] These transparency policies will be specified in each processing operation as data protection strategies by design.

In relation to security (both organisational and information security):	
	A reference to the management of the risk to rights and freedoms in the security policy applicable to the processing of personal data, as well as in the general security policy applicable to the organisation.
	An integration of the protection of rights and freedoms into the information security management system (ISMS).
	A correct differentiation of roles between the DPO and those responsible for IT or information security.
	An implementation of the necessary coordination between the DPO and the security officer of the organisation, the information system and others depending on the entity.
	A clear definition of the scope of the DPO's participation in safety committees.
	Others.
As for legal guarantees:	
	Confidentiality commitments are established for those who have access to personal data.
	Establishment of guarantees for processors that go beyond the provisions of Article 28 of the GDPR.
	Commitments are in place not to engage in efforts that could lead to the reidentification of individuals in disassociated datasets.
	Legally valid instruments are in place to protect the rights and freedoms of data subjects in the event of the materialisation of specific risks.
	Legally valid instruments are available to compensate in a balanced manner the data subjects (not the controller) for damage to their rights and freedoms in the event of the materialisation of specific risks.
	Others.
As for the training and preparation of personnel in relation to data protection:	
	Awareness and training measures are in place for personnel involved in the definition or conception of new processing
	Establishment of awareness-raising and training measures for personnel involved in personal data processing operations.
	Guides for workers, according to their specific roles, include information related to the obligations on data protection.
	Guides for workers, according to their specific roles, include information on how to deal with complaints relating to rights.
	Guides for workers, according to their specific roles, include information on what to do in the event of a personal data breach.

	Guides for workers, according to their specific roles include information regarding their rights and channels of complaint on data protection issues.
	Others.
As for the relationship between the controller and the processor	
	Model contracts include reference to clauses applicable to the relationship between the controller and the processor.
	The obligations of Article 28 of the GDPR are included in the procedures for hiring processors.
	The procedures for hiring processors include detailed procedures for assessing the processor that will ensure that only a processor will be chosen who offers sufficient guarantees to implement appropriate technical and organisational measures in accordance with the risk of the Processing[99].
	Contractual clauses shall extend beyond the requirements set out in Article 28 of the GDPR for appropriate risk management of the processing[100].
	Contractual clauses include elements that can help the processor to understand the risks to the rights and freedoms of the data resulting from the processing[101].
	The contractual clauses cover the security measures applicable to the processing.
	The contractual clauses include the obligation of the processor to obtain the approval of the controller prior to carrying out any change on security measures[102].
	The contractual clauses provide for the obligation of the controller to review these measures periodically on a risk-based basis[103].
	Additional steps to ensure compliance with personal data regulations are included in the procurement procedures.
	The controller carries out its own audits of the processors in relation to the processing.
	Independent third parties audit or certify the processor in relation to the processing.
	Others.
As for data disclosure:	
	Mechanisms are in place to have traceability of disclosure of personal data carried out by the controller and processor to processors, sub-processors and third parties.
	There are procedures with the definition of mechanisms, safeguards and limits applicable to international data transfers for each processing operation.

[99] "94. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment" Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[100] Paragraph 112 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[101] Paragraph 110 and 131 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[102] Paragraph 123 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[103] Paragraph 123 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

	There are procedures that reference to the binding corporate rules that would apply to the organisation, with details of the specific areas and processing applicable, as well as their limits.
	Others.
Within the document management policy:	
	There is a definition of documents that enable the controller to demonstrate compliance
	Includes management process of the risks posed to rights and freedoms.
	There is traceability and version control of the risk management documentation for the rights and freedoms that are generated.
	Others.
In relation to the procedures for the management of personal data breaches and processing incidents:	
	Procedures are defined to detect data breaches, incidents or errors in the processing of personal data.
	The role of the DPO is clearly defined in the procedures relating to the management of personal data breaches, ensuring, at least, that it complies with 39.1.
	There are defined procedures in place to react swiftly, at the organisational level, to breaches, incidents or errors in the processing of personal data.
	Channels of communication, information and consultation on data breaches and incidents are defined with the parties involved in the processing of personal data.
	Measures are defined to identify, in the data subjects' own communications to the controller/processor, information on breaches, incidents or errors.
	There are procedures for the notification of personal data breaches to the Supervisory Authority.
	There are procedures for communicating personal data breaches to data subjects.
	Specific scenarios of potential data breaches, errors or particularly serious incidents have been identified and the way to manage them has been defined,specifically, to protect the rights and freedoms of data subjects.
	There is a link between the procedures for the management of breaches and incidents in the processing and risk management process, including the management of associated controls.
	Others.
As for the depth of risk management:	
	Carrying out an DPIA even if it is not mandatory.
	There are internal procedures in place that make it necessary to carry out a DPIA regardless of whether or not there is a legal obligation to do so.
	Others.

Regarding monitoring and verification activities of governance measures:	
	Internal or external audit plans are in place to assess compliance with data protection policies.
	Data protection certification policies are in place.
	Where appropriate, mechanisms for adherence to codes of conduct are identified .
	Mechanisms, rules and procedures are in place to detect changes in the nature, scope, context or purposes of processing.
	Decision mechanisms are in place so that, depending on previous changes or detected incidences, a new cycle of risk review is carried out.
	Others.

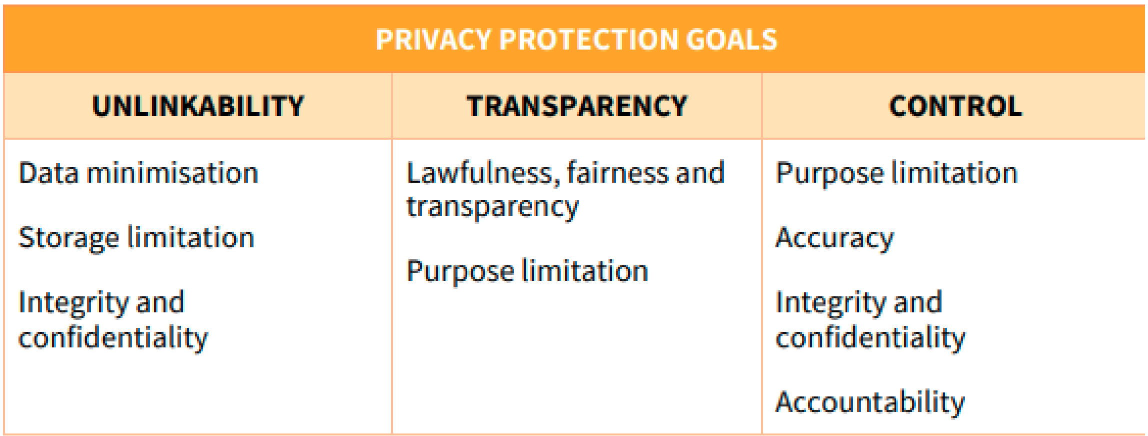
Table 37 Examples of possible Data Protection Policies and Governance Measures

C. DATA PROTECTION MEASURES BY DESIGN

Data protection controls by design are one of the measures to be taken into account in managing the risk to rights and freedoms, as set out in Article 25(1) of the GDPR.

The AEPD, in its "Guide to Privacy by Design", translates into practice the principle of data protection by design, understanding it as the need to include the protection of personal data as one of the factors to be taken into account in the specification phase of product and service requirements, together with others such as security requirements, data protection by default, accessibility or performance.

There are six objectives for the protection of personal data by design that must be taken into account for products, applications and services to be developed. On the one hand, there are the three measures aimed at protecting information security, confidentiality, integrity and availability, which are developed in the following section "Security measures for the protection of rights and freedoms". On the other hand, there are the specific ones of unlinkability, transparency and control:



PRIVACY PROTECTION GOALS		
UNLINKABILITY	TRANSPARENCY	CONTROL
Data minimisation Storage limitation Integrity and confidentiality	Lawfulness, fairness and transparency Purpose limitation	Purpose limitation Accuracy Integrity and confidentiality Accountability

Table 38 Objectives of Privacy Protection “by Design”.

The Guide to Privacy by Design contains a development of the six objectives. Here follows a brief summary of the information related to unlinkability, transparency and control.

1. Minimise

The goal of this strategy is to collect and process the least amount of data possible, thus averting the processing of unnecessary data and limiting possible impacts on privacy. This may be achieved by collecting data from fewer subjects (reducing the population size) or less data from subjects (reducing the volume of collected information), for which the following tactics may be used:

- **Select:** select only the sample of relevant individuals and the attributes required.
- **Exclude:** exclude in advance subjects and attributes that are irrelevant to the processing performed.
- **Strip**: partially eliminate personal data as soon as they cease to be necessary.
- **Destroy: completely delete personal data as soon as they cease to be relevant**.

2. Hide

This strategy focuses on limiting data observability by establishing necessary means to guarantee the protection of confidentiality and unlinkability. The following strategies are required:

- **Restrict:** restrictively manage access to personal data.
- **Obfuscate:** to make personal data unintelligible to those who are not authorised to view it.
- **Dissociate:** eliminate the link between datasets that should be kept independent, as well as the identification attributes of data records to avert correlations between them.
- **Mix:** Group together information on various subjects using generalisation and suppression techniques[104].

3. Separate

The goal of this strategy is to avoid, or at least minimise the risk while processing, within one entity, different personal data of the same individual that are used in independent processes. The measures can be:

- **Isolate:** collect and store personal data in different databases or applications that are independent, either logically or are executed on different physical systems, adopting additional measures to guarantee unlinkability.

  Another way of isolating personal data over time is the periodic renewal of unique identifiers that point to an individual.

[104] Spanish Data Protection Agency (AEPD) – Unit of Evaluation and Technological Studie. *K-anonymity as a privacy measure,* June 2019 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad-en.pdf

- **Distribute:** Spread out the collection and processing of different subsets of personal data corresponding to different types of processing over management and handling units that are physically independent within the system, and use different systems and applications to implement decentralised and distributed architectures that process the information locally whenever possible, instead of using centralised solutions with unified access which may depend on a single control unit.

4. Abstract

To limit the details of the processed personal data as much as possible. While the 'minimise' strategy makes a previous selection of the data to be collected, this strategy focuses on the degree of detail in which the data are processed and on their aggregation by using three tactics:

- **Summarise:** generalise the values of the attributes using value ranges or intervals, instead of a concrete field value.
- **Group:** aggregate information of a group of records into categories instead of using the detailed information on each of the subjects that belong to the group, by using average or general values.
- **Perturb:** use approximate values or modify the real data using some type of random noise instead of employing the exact value of the personal data.

5. Inform

This strategy aims at implementing the objective and principle of transparency beyond the minimums set by the Regulation, when the additional mechanisms are implemented to reduce risks for data subjects, as follows:

- **Supply**: to provide data subjects with additional details in relation to the processing.
- **Explain:** provide information on data processing in a concise, transparent, intelligible and easily accessible way in clear and simple language.
- **Notify:** inform data subjects particularities, incidents or changes in the nature, scope, context, purposes of the processing or in its risks, beyond the obligations set out in the GDPR.

6. Control

It aims to provide data subjects with control over the processing of their data beyond that set out in the GDPR by enabling them to manage risk, as follows:

- **Consent:** more secure mechanisms for collecting and withdrawing consent.
- **Alert:** to allow the user to determine alerts regarding the processing of his personal data.

- **Choose:** provide user control of granular functionality [105] of applications and services.
- **Update:** implement more agile mechanisms that make it easier for users to review, update and rectify data.
- **Retract:** provide mechanisms for users to delete or request deletion of personal data in a more expeditious manner.

7. Enforce

This strategy refers to the implementation, by design and in an effective manner, of procedural safeguards, policies and governance measures linked to data protection as part of the actual processing, aiming at:

- **Create:** specify data protection policies in the entity prior to the design of the processing operations and determine which ones are applicable to them.
- **Maintain:** review the effectiveness of implemented policies.
- **Uphold:** implement mechanisms in the processing to ensure policy implementation.

8. Demonstrate

The objective is the implementation of accountability policies, from the point of view of demonstrating compliance, in the processing in question. To this end, it is necessary to:

- **Record:** document any and all decisions made over time regarding processing concept, design and implementation, even if they have been contradictory, identifying who made them, when, and the rationale for doing so. The register should be supported by authenticity mechanisms such as electronic signatures or time stamps.
- **Audit:** carry out a systematic, independent and documented review of the degree of compliance with the data protection policy.
- **Report:** making such information available to the Supervisory Authority, data subjects or possible third parties, such as the supervisory body of a code of conduct, to the extent appropriate and aimed at possible risk mitigation.

PRIVACY DESIGN STRATEGY		DESCRIPTION AND TACTICS	DESIGN CONTROLS AND PATTERNS
Data oriented strategies	Minimise	Avoid unnecessary processing of personal data.	Anonymisation Pseudonymisation

[105] Functions that require consent to for their legal use must be made available separately irrespective of whether they are the main goal of the object or not.

PRIVACY DESIGN STRATEGY		DESCRIPTION AND TACTICS	DESIGN CONTROLS AND PATTERNS
		TACTICS: **select**, **exclude**, **strip** and **destroy**	Block correlation in identity management systems federated Data and metadata entry debugging
	Hide	Limit the exposure of personal data. TACTICS: **restrict**, **obfuscate**, **dissociate** and **mix**)	Access control. Selective anonymisation of access to personal data sets. Encryption Homomorphic encryption Mixed networks Attribute Based Credentials Models of zero knowledge (ZKP)
	Separate	Keep personal datasets separate. TACTICS: **isolate** and **distribute**	Anonymous black lists Physical and logical separation Data unlinking techniques
	Abstract	Limit the level of detail used in personal data processing as much as possible. TACTICS: **summarise**, **group** and **perturb**	Aggregation over time K-anonymity Noise added through obfuscation techniques Dynamic granularity. Differential privacy
Process oriented strategies	Inform	Provide extended information of the processing. TACTICS: **supply**, **explain** and **notify**	Privacy icons Processing alerts. Publish information on processing performance.

PRIVACY DESIGN STRATEGY		DESCRIPTION AND TACTICS	DESIGN CONTROLS AND PATTERNS
			Publish details of processing limitations and consequences. Publish information related to risk analysis.
	Control	Provide data subjects with effective control over their personal data. TACTICS: **consent**, **alert**, **choose**, **update**, **retract**	PIMS (personal information management systems) Privacy preferences dashboard Active broadcast of presence Credential selection
	Enforce	Application of the entity's data protection policies to the processing. TACTICS: **create**, **maintain**, **uphold**	Apply data protection policies to the processing lifecycle.
	Demonstrate	Be able to demonstrate that processing have been carried out in accordance with the entity's policies. TACTICS: **record**, **audit** and **report**.	Audit of the processing Recording and documentary control of the processing.

Table 39 Data Protection Strategies, Description, Tactics, Controls and Patterns by Design.

D. SECURITY MEASURES FOR THE PROTECTION OF RIGHTS AND FREEDOMS

Security measures for the protection of rights and freedoms are to be understood in a broad sense. That is to say, not only covering aspects relating, for example, to unauthorised access, but also other possible threats. Examples of such threats are natural causes, accidents, human error and possible errors in the operation of automated processing, in particular those arising from systems that infer new personal data or make automated decisions about individuals.

As noted in the previous sections, security requirements for the protection of rights and freedoms are part of the overall security management of an organisation (security of the organisation, people, information, continuity of processes, fight against fraud, corporate image, etc.). The selection of controls, in this case, must be guided by the need for adequate risk management for the rights and freedoms of data subjects.

In the following sections, one of the possible ways to achieve this integration will be described. However, it is recommended that security management for rights and freedoms be integrated into the entity's already established policies.

1. Processing Subject to the National Security Framework

In the case of processing operations subject to the National Security Framework (ESQUEMA NACIONAL DE SEGURIDAD - ENS) [106] the following correspondence could be made according to the level of risk to rights and freedoms determined in the processing operation:

Level of risk posed to rights and freedoms.	ENS Category
Very High	High
High	High
Medium	Medium
Low	Low

Table 40 Correspondence between the Level of Risk to Rights and Freedoms and category of the National Security Framework

This proposal is based on the experience of the Supervisory Authorities in relation to reported personal data breaches and is in no way a proposal that limits the controller who ultimately always has the obligation to implement the necessary measures to ensure the rights and freedoms of data subjects taking into account the nature, scope, context and purpose of the processing operations it carries out, as expressed in Statement WP218.[107]

2. Basic Approach to the Implementation of Security Measures

In the case of processing operations that are not subject to the obligation to comply with the ENS, the necessary measures must be implemented to manage the level of risk of the assets necessary to support the processing in each of its phases. These measures will be established and integrated in different ways according to

[106] First additional provision of the LOPDGDD: "Security measures in the public sector. 2. Controllers listed under article 77.1 of this organic law must, whenever processing personal data, implement the corresponding security measures out of those provided by the National Security Framework (ENS), as well as promote a degree of implementation of equivalent measures in those corporations or foundations linked to them and subject to private law."

[107] "Compliance should never be reduced to a checklist exercise, but rather to ensuring that personal data are sufficiently protected. The manner in which this is done may be different for each controller...... Data subjects should have the same level of protection, irrespective of the size of the organisation or the amount of data processed"

the methodology used in the organisation for information security risk management. Guidelines listing possible measures can be found in various international standards, such as ISO-27002 or in the extension for data protection issues in ISO-27701.

As a guideline, it is recommended not to implement a lower level of security than the criteria set out in Annex II of the National Security Framework, which is transferred here, in full, with the following keys (as per the Spanish):

- System category: B-basic, M-medium, A-high
- Dimension: C-confidentiality, D-availability, I-integrity, T-traceability, A-authenticity.
- "applies" indicates that a particular security measure is to be applied to one or more security dimensions.
- n.a.' means 'not applicable'.
- "=" indicates that the requirements of one level are equal to those of the level below.
- The "+" and "++" signs indicate an increase in requirements, graduated according to the lower level of the security dimension.
- Green is used to indicate that a certain measure is applied in basic or higher category systems; yellow to indicate measures that are starting to be applied in medium or higher category; red to indicate measures that are only applied in high category.
- In the list of measures, the variation from the original ENS list has been marked in red with a yellow background to reflect the obligation under articles 33 and 34 of the GDPR to manage and document personal data breaches.

Dimension	Level			**SECURITY MEASURES**	
	B	**M**	**A**		
				org	**Organisational framework**
All	applicable	=	=	[org.1]	Security Policy
All	applicable	=	=	[org.2]	Security Regulations
All	applicable	=	=	[org.3]	Security Procedures
All	applicable	=	=	[org.4]	Authorisation process
				op	**Operational framework**
				[op.pl]	Planning
All	applicable	+	++	[op.pl.1]	Risk analysis
All	applicable	+	++	[op.pl.2]	Security Architecture
All	applicable	=	=	[op.pl.3]	Procurement of new components

D	n.a.	applicable	=	[op.pl.4]	Dimensioning / Capacity Management
All	n.a.	n.a.	applicable	[op.pl.5]	Certified components
				[op.acc]	Access control.
A T	applicable	=	=	[op.acc.1]	Identification
I C A T	applicable	=	=	[op.acc.2]	Access Requirements
I C A T	n.a.	applicable	=	[op.acc.3]	Segregation of duties and tasks
I C A T	applicable	=	=	[op.acc.4]	Access rights management process
I C A T	applicable	+	++	[op.acc.5]	Authentication mechanism
I C A T	applicable	+	++	[op.acc.6]	Local access (local logon)
I C A T	applicable	+	=	[op.acc.7]	Remote login
				[op.exp]	Exploitation
All	applicable	=	=	[op.exp.1]	Inventory of assets
All	applicable	=	=	[op.exp.2]	Security Settings
All	n.a.	applicable	=	[op.exp.3]	Configuration Management
All	applicable	=	=	[op.exp.4]	Maintenance
All	n.a.	applicable	=	[op.exp.5]	Change Management
All	applicable	=	=	[op.exp.6]	Protection against malicious code
All	applicable	=	=	[op.exp.7]	Incident management
T	applicable	+	++	[op.exp.8]	Records of user activities
All	applicable	=	=	[op.exp.9]	Incident management log
T	n.a.	n.a.	applicable	[op.exp.10]	Protection of activity records
All	applicable	+	=	[op.exp.11]	Cryptographic key protection
				[op.ext]	External services
All	n.a.	applicable	=	[op.ext.1]	Contracting and service level agreements
All	n.a.	applicable	=	[op.ext.2]	Daily management
D	n.a.	n.a.	applicable	[op.ext.9]	Alternative media
				[op.cont.]	Continuity of service

D	n.a.	applicable	=	[op.cont.1]	Impact analysis
D	n.a.	n.a.	applicable	[op.cont.2]	Continuity Plan
D	n.a.	n.a.	applicable	[op.cont.3]	Periodic testing
				[op.mon]	System monitoring
All	n.a.	applicable	=	[op.mon.1]	Intrusion detection
All	applicable	+	++	[op.mon.2]	Metrics system
				mp	**Protection Measures**
				[mp.if]	Protection of installations and infrastructure
All	applicable	=	=	[mp.if.1]	Separate and access-controlled areas
All	applicable	=	=	[mp.if.2]	Identification of persons
All	applicable	=	=	[mp.if.3]	Fitting out the premises
D	applicable	+	=	[mp.if.4]	Electric power
D	applicable	=	=	[mp.if.5]	Fire protection
D	n.a.	applicable	=	[mp.if.6]	Flood protection
All	applicable	=	=	[mp.if.7]	Check-in and check-out of equipment
D	n.a.	n.a.	applicable	[mp.if.9]	Alternative facilities
				[mp.per]	Personnel management
All	applicable	=	=	[mp.per.1]	Job characterisation
All	applicable	=	=	[mp.per.2]	Duties and obligations
All	applicable	=	=	[mp.per.3]	Awareness-raising
All	applicable	=	=	[mp.per.4]	Training.
D	n.a.	n.a.	applicable	[mp.per.9]	Alternative personnel
				[mp.eq]	Protection of equipment
All	applicable	+	=	[mp.eq.1]	Uncluttered workstation
A	n.a.	applicable	+	[mp.eq.2]	Workplace blocking
All	applicable	=	+	[mp.eq.3]	Protection of portable equipment
D	n.a.	applicable	=	[mp.eq.9]	Alternative media

				[mp.com]	Protection of communications
All	applicable	=	+	[mp.com.1]	Secure perimeter
C	n.a.	applicable	+	[mp.com.2]	Confidentiality protection
I A	applicable	+	++	[mp.com.3]	Protection of authenticity and integrity
All	n.a.	n.a.	applicable	[mp.com.4]	Segregation of networks
D	n.a.	n.a.	applicable	[mp.com.9]	Alternative media
				[mp.si]	Protection of information media
C	applicable	=	=	[mp.si.1]	Tagged
I C	n.a.	applicable	+	[mp.si.2]	Cryptography
All	applicable	=	=	[mp.si.3]	Custody
All	applicable	=	=	[mp.si.4]	Transport:
C	applicable	+	=	[mp.si.5]	Deletion and destruction
				[mp.sw]	Protection of software
All	n.a.	applicable	=	[mp.sw.1]	Development
All	applicable	+	++	[mp.sw.2]	Acceptance and commissioning
				[mp.info]	Protection of information
All	applicable	=	=	[mp.info.1]	Personal data
C	applicable	+	=	[mp.info.2]	Qualification of information
C	n.a.	n.a.	applicable	[mp.info.3]	Encryption
I A	applicable	+	++	[mp.info.4]	Electronic signature
T	n.a.	n.a.	applicable	[mp.info.5]	Time stamps
C	applicable	=	=	[mp.info.6]	Cleaning of documents
D	applicable	=	=	[mp.info.9]	Backups.

				[mp.s]	Protection of services
All	applicable	=	=	[mp.s.1]	Protection of electronic mail
All	applicable	=	+	[mp.s.2]	Protection of web services and applications
D	n.a.	applicable	+	[mp.s.8]	Denial of service protection
D	n.a.	n.a.	applicable	[mp.s.9]	Alternative media

Table 41 Selection of Security Measures.

3. Management of Personal Data Breaches.

The management of personal data breaches must be sized according to the risk to rights and freedoms. Specific controls aimed at ensuring proper detection and management of the breach could include:

Specific Controls in the management of Personal Data Breaches
Contingency plans for a personal data breach.
Establishment of technical resources for the automatic detection of personal data breaches.
Incident management tools adapted to the requirements of the GDPR.
Protocols for the identification of potential breaches in user or data subjects complaints or communications.
Ability to assess the severity of the data breach.
Procedures for accurately describing the impact of a data breach on rights and freedoms.
Agile internal channels for communication of the data breach to the DPO, if appointed.
Agile channels of communication between the controller and the processor regarding the data breaches.

Procedure for deciding how to act in relation to the protection of rights and freedoms in the face of the breach.
Procedures for notifying the Supervisory Authority in order to comply with the requirements of Article 33.
Procedures for communication to data subjects in order to comply with the requirements of Article 34.

Table 42 Specific Controls in the processing of Personal Data Breaches.

4. Resilience

Specific controls aimed at implementing an adequate degree of resilience of personal data and the systems that support them could include the following:

Target	Controls
People capability	Ability to detect changes
	Ability to communicate them
	Ability to understand them
	Ability to innovate
	Ability to act in real time
	Willingness to act proactively
Adequate flow of information	Agile
	Specific
	Minimum
	Complete
	From and to the right people
Leadership	Clear points of decision making Well-defined responsibilities.
Strategic adaptability	Physical, technological and organisational structures need to be able to evolve in real time towards new objectives or ways of acting.

Table 43 Resilience-Related Controls.

5. Failures in Technical Data Protection Safeguards and Application Errors

Measures in the case of breaches of technical data protection safeguards, such as pseudonymisation, as well as possible errors in applications, can be projected in the following measures as follows:

Dimension	Level			SECURITY MEASURES	
	B	M	A		
				org	Organisational framework
F,E	applicable	=	=	[org.4]	Authorisation process
				op	Operational framework
				[op.pl]	Planning
F,E	applicable	+	++	[op.pl.1]	Risk analysis
F,E	n.a.	applicable	++	[op.pl.5]	Certified components
				[op.exp]	Exploitation
F,E	n.a.	applicable	=	[op.exp.3]	Configuration Management
F,E	applicable	=	=	[op.exp.4]	Maintenance
F,E	n.a.	applicable	=	[op.exp.5]	Change Management
F,E	applicable	=	=	[op.exp.7]	Incident management
F,E	applicable	=	=	[op.exp.9]	Incident management log
				[op.ext]	External services
F,E	n.a.	applicable	=	[op.ext.1]	Contracting and service level agreements
F,E	n.a.	applicable	=	[op.ext.2]	Daily management
				[mp.per]	Personnel management
F,E	applicable	+	++	[mp.per.3]	Awareness-raising
F,E	applicable	+	++	[mp.per.4]	Training.
				[mp.sw]	Protection of computer applications
F,E	applicable	+	++	[mp.sw.1]	Development
F,E	applicable	+	++	[mp.sw.2]	Acceptance and commissioning

Table 44 Controls relating to Failures in the Technical Safeguards for Data Protection and Errors in Applications

6. Advanced Approach to the Implementation of Security Measures

A more detailed management on security risk management could be done on the basis of a complete analysis of each of the assets identified in the processing. In this case, each of the security dimensions affected for each asset would be analysed (check the section Identification and analysis of risk factors -> Risk arising from personal data breaches -> Complete analysis), applying the most appropriate specific controls for each of the assets, according to their level of risk and the category in which they fall.

Based on the category established for each asset, these would be implemented for that particular asset. For each identified threat, one or more controls should be established taking into account the characteristics of the asset to be protected, as well as the cost of the control(s) to be implemented.

In this case, it is recommended to apply the criteria followed for the system for managing the entity's information systems.

IX. RESIDUAL RISK ASSESSMENT AND REVIEW

A. ASSESSING RESIDUAL RISK

The level of risk of the processing must be assessed before implementing the measures, in order to determine the level of intrinsic risk. However, it also needs to be recalculated after risk mitigation measures and safeguards have been put in place. In this regard, it will be possible to determine whether the risk has been reduced to the desirable threshold. This is the way in which measures are to be implemented and the residual risk is to be calculated until it reaches acceptable levels.

Similarly, if the nature, scope, context or purposes of the processing are altered, it will be necessary to carry out the assessment again.

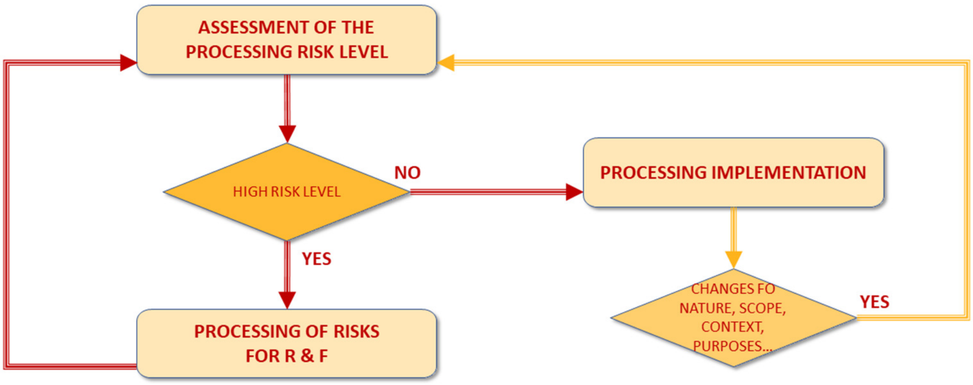

ASSESSMENT OF THE PROCESSING RISK LEVEL
HIGH RISK LEVEL
NO
PROCESSING IMPLEMENTATION
YES
CHANGES FO NATURE, SCOPE, CONTEXT, PURPOSES...
YES
PROCESSING OF RISKS FOR R & F

Figure 28: Risk Assessment Cycle.

Each risk factor may entail several associated controls (measures and/or safeguards) assigned to reduce its level of risk and, for each of these controls, the effectiveness must first be assessed individually and, then, in aggregate.

These can influence the likelihood and/or impact of a potential threat and their effectiveness can be assessed on the basis of one's own or others' experience with such controls. On the other hand, the same control can reduce the level of risk for more than one risk factor.

The effectiveness value (aggregate effectiveness) shall be determined for each identified risk factor, classified into the following levels:

- **Negligible or limited effectiveness**: The likelihood and impact of the threat shall not be affected by the implementation of the controls; they remain largely unchanged or vary slightly. The risk level of the risk factor shall not be reduced.
- **Relevant effectiveness**: The likelihood and impact of the threat are significantly reduced. In that case, the new risk level shall be estimated.
- **Maximum effectiveness**: The likelihood and/or impact of the hazard is drastically reduced to negligible or close to negligible values. The risk level of the risk factor shall be reduced to low.

The effectiveness of the identified controls will result in an assessment of the residual risk level. If in the first step, the risk level of the processing has been calculated from the intrinsic risk levels for each risk factor, in this phase of risk management it is calculated from the residual risk levels.

Risk factor	Intrinsic risk level	Controls and their characteristics	Residual risk level.
Factor 1	Intrinsic level 1	Control 1	Residual level 1
		Control 2	
		…	
..			
Factor N	Intrinsic level N	Control M	Residual level N
		Control M+1	
		…	
	Intrinsic risk level of the processing operation		**Residual risk level of the processing operation**

Table 45 Assessment of Residual Risk vs. Intrinsic Risk.

B. ASSUMABLE RISKS

As noted above, there is no such thing as "zero risk". A compromise has to be found between the level of residual risk achieved and the feasibility of processing, which means making a decision as to when a level of risk is acceptable.

Without prejudice to the obligations of the controller, low and medium levels of residual risk that shall require proportionate management efforts throughout the lifecycle of the processing could be considered as acceptable levels of residual risk.

This means that if the controller, during the analysis, determines that the processing has a residual risk level of higher than medium value, this party shall have to take further measures and safeguards necessary to manage the identified risks. Once designed to be incorporated into processing, in an iterative process, reassess the level of risk and repeat the process until the residual level of risk is acceptable.

As expressed in the WP248 Guidelines: "An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a wellknown vulnerability is not patched)."

If the entity merely "adjusts" its assessment so that the result obtained is close to its own interests, then the risk factors have not been properly addressed, and the controller will be held liable.

C. REVIEW OF THE LEVEL OF RISK

In order to determine when to conduct a review in the risk management process of an ongoing processing, rather than setting time frames, it is necessary to identify those circumstances that should be used as triggers for such a review.

These events will change the nature, scope, context or purpose of the processing. The following table provides some examples of factors that could be used to determine when a risk level review is necessary:

Elements that trigger a risk management review cycle	
Nature	• Changes in the identity of the controller. • Changes in processing implementation. • Changes or upgrades of technological elements. • Replacing human elements for technical elements. • Substantial changes in organisational elements. • Substantial changes in processing orders. • Detection of lack of effectiveness in the measures and guarantees included in the processing.
Scope	• Change in the processing extent. • Change in the categories of data collected. • Change in the volume of data collected. • Change in the frequency of data collection. • Change of scope (temporal or spatial).
Context	• Major changes in the organisation's purposes, governance models or culture. • Change in the situations that justified the processing operations. • Incidents and breaches that have occurred in processing or similar processing operations. • Evolution of the threat model, incidents, data breaches or applicable technologies. • Changes in the volume or typology of requests in the exercise of the rights of data subjects. • Changes in legal frameworks or guarantees. • Changes in the regulatory implementation framework. • Corporate, political, economic or strategic changes.
Purposes	• Change or extension of the primary or secondary purposes of processing.

Table 46 Elements triggering a risk management review cycle.

These changes may mean that the level of risk decreases as well as increases, even to the point of making it mandatory to carry out an DPIA.

SECTION 3: DATA PROTECTION IMPACT ASSESSMENT

X. THE DATA PROTECTION IMPACT ASSESSMENT

DPIA and risk management are integrated activities. The DPIA is an indivisible part of risk management for rights and freedoms and has to be implemented within the framework of this risk management.

The data protection impact assessment has been introduced in the section 'Risk management for rights and freedoms and the DPIA' in the chapter 'Items associated with risk management'.

The following items have been described in more detail in this section:

- The DPIA is mandatory when there is a likelihood of high risk in processing operations.
- The DPIA is a process.
- The DPIA is integrated into risk management for rights and freedoms.
- The DPIA extends risk management requirements.
- The DPIA has to be translated into positive actions for the implementation of risk management measures and safeguards.
- The DPIA is also a tool for demonstrating compliance.

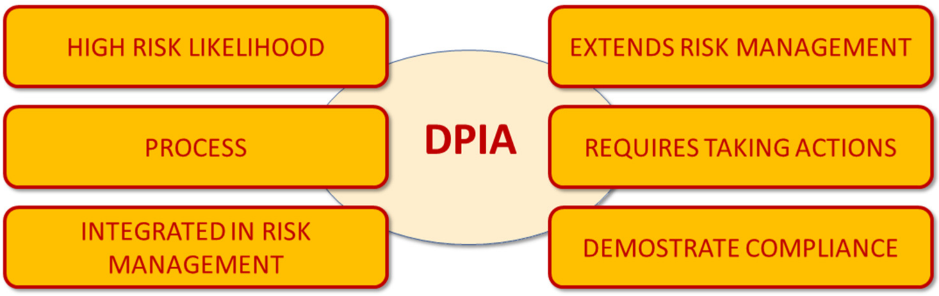


Figure 29: Basic features of the DPIA

All chapters prior to this section are required and are part of the DPIA. The following chapters develop the specificities of the DPIA.

A. WHO CONDUCTS THE DPIA

The DPIA is a specific obligation of the controller, as set out in Article 35(1). This implies that the latter assumes the responsibilities arising from its implementation and the results it produces.

As interpreted in the WP248 Guidelines:

> *"Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.*

> *The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.*
>
> *If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information."*

Therefore, processors have the obligation to assist the controller in ensuring compliance with the obligations set out in Articles 32 to 36, i.e. in risk management and in the performance of the DPIA, taking into account the nature of the processing and the information available to the processor (Art. 28.3.f). In addition, it may be advisable for the controller to seek support from third parties.

B. WHEN IS THE DPIA CARRIED OUT

With regard to the time at which this must be done, Article 35(1) of the GDPR provides that:

> *... the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ...*

The DPIA is a process that is integrated into the risk management process for rights and freedoms itself. Within this management process, an important aspect of the DPIA is its *a priori* character, i.e. the obligation to implement it before the start of the processing activities.

The GDPR stresses this prior nature in relation to the actual execution of the processing. It explicitly does not require that this be done prior to other stages of the processing lifecycle, such as design or implementation. In this regard, the GDPR is limited to the exercise of its powers, i.e. it does not go into other considerations beyond the protection of personal data. The rights and freedoms of citizens will be affected when the processing is actually carried out. Therefore, it is before these rights and freedoms are compromised that the DPIA should be carried out.

However, although the GDPR does not enter into the assessment, it would be highly advisable for the entity to carry out the DPIA before starting the actual design and implementation process. Every phase of the development lifecycle of a processing prior to its operation involves investments in development, procurement, organisational changes, contracting, etc. In this regard, the WP248 Guidelines literally express themselves in the following terms:

> *"The DPIA should be seen as a tool for helping decision-making concerning the processing"*

It follows that it is advisable to carry out the DPIA at the conception and design stages of the processing. There are two reasons for this approach. The first is to protect the investment made by the controller in processing, but this reason does not fall under data protection competences.

The second is to comply with data protection principles by design. These principles require that the selected safeguards are guided by risk management and are implemented during the conception and design phase of the processing, integrated into the processing and extending to all stages of its life cycle. Data protection by design is not an additional layer or an element that can be added afterwards[108]. Therefore, a DPIA, which may imply that changes need to be made to the processing in order to introduce modifications, safeguards or risk mitigation measures, has to be carried out before and during the design phase.

C. EXCEPTIONS FOR CARRYING OUT THE DPIA PRIOR TO THE START OF PROCESSING ACTIVITIES

The risk approach of the GDPR assumes that the DPIA should be understood as a process and not as a state. Therefore, while the DPIA must be conducted prior to the implementation of the processing, its review and adaptation extends to all stages of the processing lifecycle.

If, during the lifetime of the processing, changes occur outside the controllers' control, such as contextual changes or an unplanned extension of the scope/scope, it will be necessary to update the DPIA and, where appropriate, generate a new report and action plan with the additional control measures that need to be implemented within the framework of risk management before continuing with the processing. If the DPIA had not been conducted because the initial circumstances did not compel or recommend it, then the DPIA would need to be conducted from scratch. In the above cases, the DPIA must be implemented immediately.

If the controller intends to change the nature, scope or purposes of the processing, and the new circumstances require or recommend a DPIA, the DPIA must be carried out prior to the start of processing activities with the new updates.

Among the above cases, it must be noted those processing operations that were already in progress before the full entry into force of the GDPR. With regard to the latter case, it should be noted that the WP248 Guidelines state:

> *... even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.*

It is therefore the obligation of the controller to carry out a risk level review for processing operations already in progress (check the chapter on risk level review) in order to determine the appropriate moment to carry out the DPIA.

[108] The GDPR does not deal with data protection AFTER design.

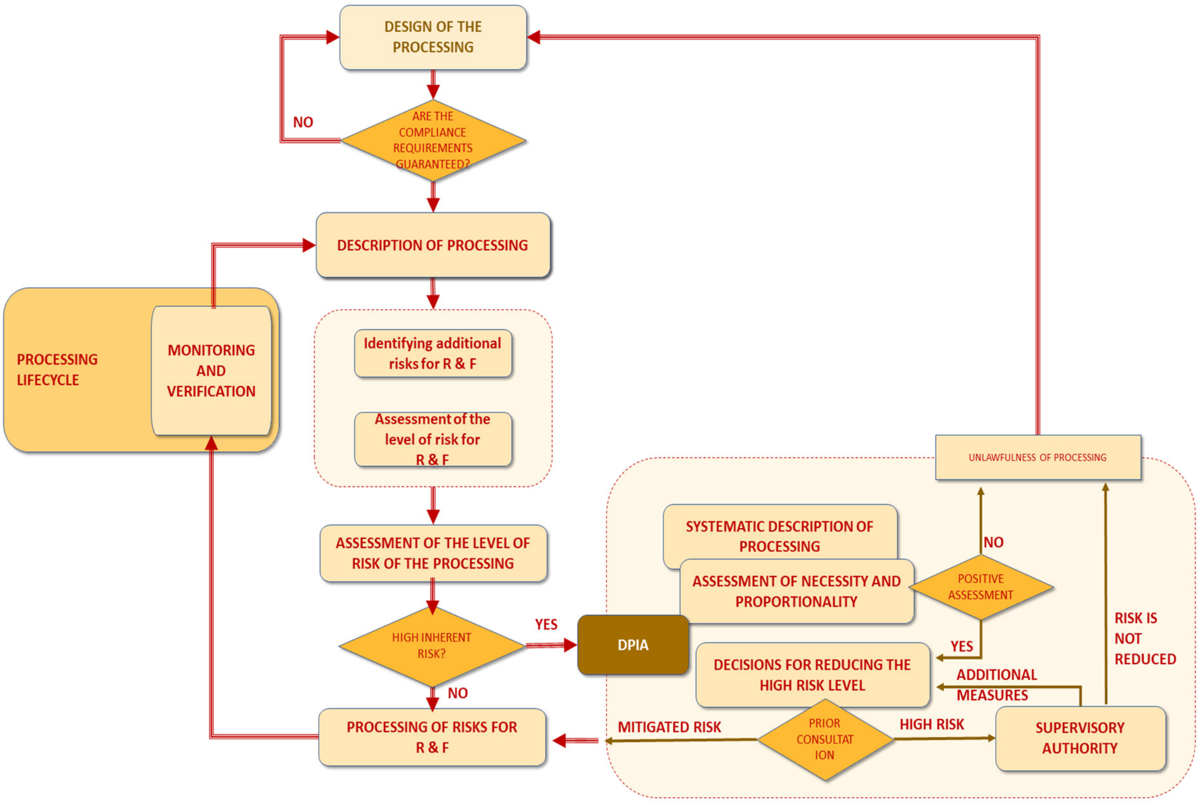

DESIGN OF THE PROCESSING
NO
ARE THE COMPLIANCE REQUIREMENTS GUARANTEED?
DESCRIPTION OF PROCESSING
PROCESSING LIFECYCLE
MONITORING AND VERIFICATION
Identifying additional risks for R & F
Assessment of the level of risk for R & F
ASSESSMENT OF THE LEVEL OF RISK OF THE PROCESSING
HIGH INHERENT RISK?
YES
NO
DPIA
PROCESSING OF RISKS FOR R & F
UNLAWFULNESS OF PROCESSING
SYSTEMATIC DESCRIPTION OF PROCESSING
ASSESSMENT OF NECESSITY AND PROPORTIONALITY
NO
POSITIVE ASSESSMENT
YES
RISK IS NOT REDUCED
DECISIONS FOR REDUCING THE HIGH RISK LEVEL
ADDITIONAL MEASURES
MITIGATED RISK
PRIOR CONSULTAT ION
HIGH RISK
SUPERVISORY AUTHORITY

Figure 30: DPIA in the risk management process.

XI. ANALYSIS OF THE OBLIGATION TO CARRY OUT A DPIA

The analysis of the obligation to conduct a DPIA is part of the process of assessing the risk to rights and freedoms. This process has been described in the previous chapters, although, in order to facilitate the reading of the text, this analysis has been separated into a separate chapter.

A. WHEN A DPIA IS NOT MANDATORY

A DPIA is not required, without prejudice to other obligations under the GDPR, where the processing:

- "is not likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1));
- It falls within the scope of the Indicative list of types of processing which do not require a data protection impact assessment in accordance with Article 35.5 of the GDPR published by the AEPD and validated by the EDPB.
- Where the nature, scope, context and purposes of the processing are very similar to the processing for which a prior DPIA has been carried out. In such cases, the results of such a DPIA conducted for similar processing operations may be used (Article 35(1));
- Where a processing activity, pursuant to Article 6(1)(c) or (e), has a legal basis in European Union law or Member State law, where that law regulates the specific processing operation and where a DPIA has already been carried out in the context of the adoption of that legal basis (Article 35(10)), except where a Member State considers it necessary to carry out such an assessment prior to the specific processing activities to be regulated;
- Where the processing activities have been verified by the Supervisory Authority before May 2018 under specific conditions that have not changed (check III.C);

B. WHEN A DPIA IS MANDATORY

The conditions for considering that the controller is obliged to carry out a DPIA of the processing are determined as follows:

OBLIGATION TO CARRY OUT THE DPIA
"Where a type of processing, in particular if it uses new technologies, is likely, by its nature, scope, context or purposes, to result in a high risk to the rights and freedoms of natural persons" [109]
It falls within one of the cases set out in Article 35.3 of the GDPR.
There is a special rule requiring an DPIA for processing.
Where the processing corresponds to one of the examples of obligation listed in the WP248 Guidelines.
When the processing meets at least two of the conditions listed in the WP248 Guidelines for conducting a DPIA.
Where the processing meets two or more of the criteria of the *list of the kind of processing operations which are subject to the requirement for a data protection impact assessment (art 35.4)* published by the AEPD.
When a high risk has been assessed taking into account the cases listed in Article 28.2 of the LOPDGDD.
Where in any of the guidelines issued by the EDPB, the processing is identified as being required to carry out a DPIA.
The processing is subject to a code of conduct or a certification mechanism requiring the controller to carry out an impact assessment.

Table 47 Obligation to carry out the DPIA

The assessment of these conditions must be made on the basis of the description of the processing and the risk factors identified in the risk analysis process for rights and freedoms. The assessment of risk has been developed in the chapter "Assessing the level of risk of processing".

The WP248 Guidelines interpreted that for processing operations in progress at the time of the entry into force of the GDPR that had already been reviewed by the Control Authority or by the DPO it was not mandatory to carry out the DPIA.

However, the same WP248 Guidelines set forth that:

> *"Data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA".*

Taking into account that at the time of publishing this guide more than three years have passed since the full entry take effect of the GDPR, and because of the potential evolution in the nature, context and even the scope to which the processing operations are subject, in line with the controller's obligation to review and update the measures when necessary[110], it is recommended to carry out a DPIA for those high-risk processing operations that

[109] Article 35(1) of the GDPR and Recital 76

[110] Article 24.1 GDPR

at the time, did not do so on the basis of the above exception. Not carrying out any review or not carrying out the DPIA of these processing operations *sine die* cannot be understood, in any case, as a way of demonstrating compliance with the provisions of the GDPR in relation to the active accountability framework.

XII. ANALYSIS OF THE NEED TO CARRY OUT A DPIA

The set of mandatory processing operations is neither a closed list nor a limitation for the controller. Sometimes it may be necessary or advisable to conduct a DPIA for a processing operation that is not on the list of required processing operations, either because of the potential intrinsic risk that the controller has identified in the processing operation, because the controller implements the DPIA as a tool to demonstrate compliance or, as stated in the WP248 Guidelines, it is unclear whether or not a DPIA is required:

> *In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.*

And as stated in the Guidelines, when, although not all the criteria for a mandatory DPIA are met, some of them are met to such an extent that the controller considers it necessary to carry out the DPIA:

> *However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.*

Therefore, it is important to bear in mind that the fact that a processing of personal data does not fall within the mandatory cases does not always imply that it is not necessary to carry out the DPIA. The GDPR does not limit the controller's ability to decide whether or not to carry it out. The GDPR establishes a mechanism of proactivity that allows the controller to decide on the need to carry out the DPIA in line with the inherent risks associated with the processing in accordance with its nature, scope, context and purposes (Recital 76 and Article35.1 of the GDPR).

In particular, it should be noted that the lists of required and excluded processing operations established by the supervisory authorities and referred to in Article 35 of the GDPR (35.4 and 35.5) are indicative and do not limit the controller's power to decide on its processing of personal data and on the exercise of proactive accountability.

In particular, the WP248 Guidelines set forth:

> *the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;*
>
> *the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.*

Hence, both the DPO, or if not appointed the data protection advisor, and the CISO may suggest that a DPIA be carried out. These suggestions should be documented, as well as the decisions taken on the basis of them.

Therefore, irrespective of whether or not a processing operation is required to conduct a DPIA, the controller may decide to conduct a DPIA in order to carry out a more detailed analysis of the processing of personal data in the interest of greater diligence in implementing proactive accountability. They are also valid reasons to improve the quality of your products and services, to foster a culture of data protection in your organisation or simply as a mechanism to ensure the trust of your customers.

XIII. ASSESSMENT OF THE NECESSITY AND PROPORTIONALITY OF THE PROCESSING

One of the requirements of Article 35 of the GDPR in relation to the DPIA is the one set forth in paragraph 35.7.b of the GDPR, the obligation to carry out *"an assessment of the necessity and proportionality of the processing operations in relation to the purposes".*

The European Data Protection Supervisor has published two guidelines to carry out such an analysis in relation to European regulatory developments[111]. Although they are not directly applicable to the analysis of any possible type of processing, they are very useful in providing the basis for the assessment of necessity and proportionality[112]. They specify the principle of proportionality followed by judges and courts[113] when weighing different legally protected rights or assets in conflict.

This principle of proportionality, taken to the assessment of the necessity and proportionality of the processing, translates into a weighting based on three criteria:

Judgement of suitability	It must be determined whether the processing is fit for purpose. Processing responds to certain objective deficiencies, demands, requirements, obligations or opportunities and can meet the following purposes proposed with sufficient effectiveness.
Judgement of necessity	It must be determined whether the intended purpose cannot be achieved in another less harmful or invasive way, i.e. there is no alternative processing that is equally effective in achieving the intended purpose.

[111] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.

[112] Recital 4 GDPR: *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."*

[113] The Constitutional Court has pointed out in its STC14/2003, of 28 January, FJ9 that *"in order to verify whether a measure restricting a fundamental right passes the test of proportionality, it is necessary to ascertain whether it meets the following three requirements or conditions: whether such a measure is likely to achieve the proposed objective (judgement of suitability); whether, furthermore, it is necessary, in the sense that there is no other more moderate measure for the achievement of such a purpose with equal effectiveness (judgement of necessity); and, finally, whether it is balanced, as it derives more benefits or advantages for the general interest than harm to other conflicting goods or values (Judgement of proportionality in the strict sense)"*

Judgement of proportionality in the strict sense	The seriousness of the risk to rights and freedoms, and its intrusion into privacy, must be appropriate to the aim pursued and proportionate to the urgency and severity of the processing. The benefit that the processing, from a data protection point of view[114], provides to society has to be weighed against the impact on other fundamental rights. However, even if it may partially give way, in no case can one assume the absolute denial of the right to data protection and empty it of its essential content.

Table 48 Judgement of Suitability, Necessity and Proportionality in the Strict Sense.

This assessment should result in a decision whether or not to carry out the processing or, if necessary, to modify it so that it complies with the three required judgements.

During the assessment process, some elements can be identified and, when included in the processing operation, they may modify it and make it conform to the principle of proportionality, so this assessment and adequacy process should be understood as a process of improvement that can and should be carried out in several iterations until an adequate processing design is achieved.

Before tackling this assessment from scratch, it is essential to consult the necessity and proportionality analyses that may have been carried out previously on similar processing operations, consult the EDPB guidelines, the AEPD's resolutions or legal reports, or case law, where there may be assessments of processing operations that are similar in terms of the nature, scope, context or purposes of the processing and which allow the limits to which the processing operation in question must be addressed to be identified. The findings of these assessments need to be taken into account throughout the assessment.

In no case is it recommended to proceed with the DPIA when the processing does not pass the necessity and/or proportionality assessment. Please note that these are compliance requirements under the GDPR; requirements that cannot be addressed by alternative measures to compliance itself, such as technical and organisational measures.

For practical application, this guide proposes a sequential analysis process, starting with the judgement of appropriateness. This process should be adjusted by the controller to his or her working methodology and to the characteristics and particular circumstances of the specific processing. The only requirement is that a full analysis of all three dimensions is carried out.

[114] Recital 4: "The processing of personal data should be designed to serve mankind.. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality..."

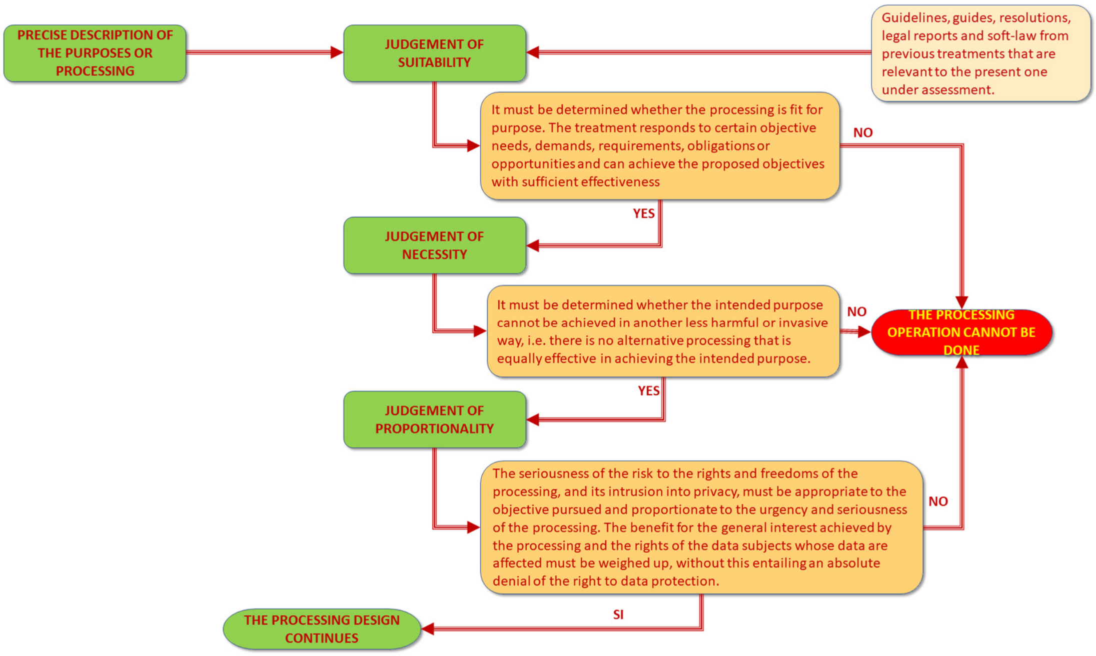

PRECISE DESCRIPTION OF THE PURPOSES OR PROCESSING
JUDGEMENT OF SUITABILITY
Guidelines, guides, resolutions, legal reports and soft-law from previous treatments that are relevant to the present one under assessment.
It must be determined whether the processing is fit for purpose. The treatment responds to certain objective needs, demands, requirements, obligations or opportunities and can achieve the proposed objectives with sufficient effectiveness
NO
YES
JUDGEMENT OF NECESSITY
It must be determined whether the intended purpose cannot be achieved in another less harmful or invasive way, i.e. there is no alternative processing that is equally effective in achieving the intended purpose.
NO
THE PROCESSING OPERATION CANNOT BE DONE
YES
JUDGEMENT OF PROPORTIONALITY
The seriousness of the risk to the rights and freedoms of the processing, and its intrusion into privacy, must be appropriate to the objective pursued and proportionate to the urgency and seriousness of the processing. The benefit for the general interest achieved by the processing and the rights of the data subjects whose data are affected must be weighed up, without this entailing an absolute denial of the right to data protection.
NO
SI
THE PROCESSING DESIGN CONTINUES

Figure 31: Process of Assessing Necessity and Proportionality.

The measures that the controller is obliged to review and update (Article 24(1)) will include the assessment of the judgement of appropriateness, necessity and proportionality, carrying out the objective quantification of the results of the processing and the application, where it exists, of the corresponding sunset clauses.

A. COMMON MISUNDERSTANDINGS REGARDING THE ASSESSMENT OF THE NECESSITY AND PROPORTIONALITY OF PROCESSING

During the practical implementation of the GDPR, the following misunderstandings have been observed in relation to the assessment of necessity and proportionality of processing.

Firstly, the DPIA is an analysis in the framework of risk management for rights and freedoms, and does not aim to determine the legitimacy of the processing or its legal bases.

Secondly, this assessment should not be confused with the analysis of the need for a DPIA (check chapter "Analysis of the need for a DPIA"), which will depend on the level of risk of the processing that has been identified.

Finally, it should be noted that the assessment of the proportionality of processing operations in relation to their purposes (Article 35(7)(b) GDPR) should not be confused with the controller's obligation to use only data that are adequate, relevant and limited to the purpose of the processing (Article 5(1)(b) and Article 25(2) GDPR). Article 5(1)(b) and Article 25(2) of the GDPR require the controller to carry out an analysis exercise aimed at applying the minimisation principle and which involves determining, for each of the operations constituting the processing, the minimum data and processing operations necessary to achieve the purposes of the processing.

B. JUDGEMENT OF SUITABILITY

The judgement **of suitability** must assess whether the processing proposal, as it stands, is effective enough to achieve its intended purpose. Such effectiveness must necessarily be objectively demonstrated by the controller, for which purpose, the following must be carried out:

1. Definition of the threshold of processing effectiveness: Establishing, in an objective, qualitative and evidence-based way, what threshold of effectiveness should be achieved to meet the purposes of the processing (examples could be a 5% margin of error on a result value, 95% case detection or a chance of fraud below 1%).
2. Evaluation of the effectiveness of the processing proposal: Assessing, in an objective, qualitative and evidence-based way, the effectiveness of the processing as it has been proposed, verifying whether it responds to the needs raised and to what extent (to determine whether it genuinely resolves these shortcomings).

The judgement of suitability must be rational, analytical and based on objective facts and data.

Based on the information obtained in this analysis, a decision will be made whether or not to proceed with processing as planned.

C. JUDGEMENT OF NECESSITY

The following steps must be taken in order to carry out the judgement of necessity:

1. Determination of the relevance of the purposes of the processing: Assessing that the purposes of the processing are of sufficient importance to be addressed by high-risk processing (subject to a proportionality judgement described below).
2. Verification of the suitability of processing operations: Verification that each of the specific processing operations is aimed at fulfilling the purposes of the processing in an objectively demonstrable manner.
3. Justification of the current processing setting: Assessing that there are no other processing, already underway or that could be considered, that meet the stated purposes without incurring a high risk, even if some modification is necessary to meet the stated purposes.

In practice, there is usually no single way to meet the purposes for which a data processing operation is intended. Depending on how this is implemented, different risk scenarios can be envisaged. When considering these other possible alternative processing, it is necessary to identify those that, using less intrusive means, achieve at least equal effectiveness.

In other words, it must be assessed whether the purpose pursued can be achieved by other means, such as, for example, using other data (of a different nature, extent or anonymised), reducing the universe of affected persons (quantitatively or qualitatively speaking), making use of other less invasive technologies, applying other procedures or means of processing (modifying those initially planned), etc. and even determining whether minor modifications to the existing processing operations cover the needs identified in the first point.

Once this assessment has been made, the alternative must be chosen which, while achieving the necessary effectiveness, is the least damaging and intrusive to the rights of individuals. Ultimately, the decision will be made whether or not to proceed with processing as planned.

1. Validity clauses

A very important aspect of the necessity analysis is that it has to be determined whether the justification for the processing is based on the requirement to respond to a specific emergency situation (e.g. in case of an essential public interest such as security or health issues, in which case it would have to be laid down in a law). In this case, it is essential to identify whether there is a high risk for the responsible party, the State or the public (a risk other than a risk to the rights and freedoms of the data subjects) and, in particular, for those groups of citizens who could be considered to be particularly vulnerable.

The weighing of circumstances has to be done on a case-by-case basis and according to the circumstances of the moment, as there are no absolute rights and no absolute limits to them. Precisely because these limits may vary over time as a result of the evolution and change of the conditions that have imposed them, it is necessary to establish, in the case described above and in other similar cases that may be identified, the so-called "validity clauses" for processing, understood as those circumstances that may occur and make the processing unnecessary depending on its nature, scope, context and purposes.

In such cases, the controller has to incorporate measures to monitor the actual circumstances that justified the processing. In the event that these no longer exist, the appropriateness and lawfulness of the processing must be reassessed (Article 6 GDPR). Therefore, processing based on provisional measures aimed at responding to an extraordinary situation of urgent need will be prevented from becoming permanent, definitive and unjustified.

D. JUDGEMENT OF PROPORTIONALITY IN THE STRICT SENSE[115]

At the time of making the judgement of proportionality in the strict sense, based on the above analyses, and once the suitability and necessity of the processing has been objectively and justifiably accredited, it is necessary to carry out the following:

1. Identification of the degree of impact of the processing on rights and freedoms: Expressing, in detail, the limitations or encroachments on the rights and freedoms of the

[115] Recital 4. "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

rights and freedoms that the processing may entail for the data subject. This assessment is a previous task that has already been carried out in the determination of the risk factors and levels previously analysed (check chapter "Identification and analysis of risk factors"), and at this point in the assessment, the conclusions are set out.

2. Identification and description of compensatory measures: Detailing the controls put in place in the processing design to mitigate the impact.
3. Identification of the benefits of processing: Determining the evidenced benefits and advantages of processing for individual and collective stakeholders. In other words, the social benefit must also be considered.
4. Confirmation of the existence of identity in the quality of the information used: It has to be assessed whether there is symmetry in the information analysed for the weighting judgement, i.e. whether the level of analysis in relation to impact is equal to the level reached on the basis of the information provided in relation to benefits.
5. BHB (Benefit-Harm Balance) analysis: Assessing whether the previously determined benefits for data subjects and society outweigh and justify the impact on the rights and freedoms identified in point 1 of this proportionality test in the strict sense.

One aspect of determining that the DPIA is incomplete is if there is an asymmetry between the information provided in relation to the constraints posed by the processing and the information provided in relation to the benefits it brings, for example, attempting to justify the necessity of the processing solely in terms of business interests without taking into account the rights and freedoms of data subjects in particular and of society in general.

E. PARTICULAR CASE OF PROCESSING: NECESSITY AND PROPORTIONALITY IN REGULATORY DEVELOPMENT

In the event that the DPIA is carried out on a legislative initiative that proposes a limitation of rights (Article 35.10 GDPR), the analysis carried out to assess the necessity and proportionality of the processing on the basis of the judgements described above, in particular those of appropriateness and necessity, takes on greater importance in view of the scope and degree of impact that the processing entails[116].

F. FINAL DECISION AND DOCUMENTATION OF THE ASSESSMENT OF NECESSITY AND PROPORTIONALITY

The assessment of necessity and proportionality should lead to a decision as to whether the processing is feasible or, on the contrary, not feasible in the form in which it is proposed.

Where it is not possible to demonstrate the necessity and proportionality of a high-risk processing operation or of the processing operations that could form part of it, it is not recommended to proceed with the data protection impact assessment or even to carry out the prior consultation referred to in Article 36 of the GDPR. The

[116] Some examples of DPIA in this context can be found at the following link https://ec.europa.eu/transparency/documents-register/ r

accountability tools do not serve to justify, in any case, the necessity and/or proportionality of the processing.

Where it is concluded that the processing is not necessary or not proportionate, the issues leading to this conclusion should be identified and, if possible, the necessary modifications should be made to bring the processing into line with the appropriate criteria of necessity, suitability and proportionality.

In the process of conducting the necessity and proportionality assessment, it is necessary to provide appropriate evidence, record and store all relevant information for this analysis, and report the entire assessment process and its conclusions in a report.

As has been repeatedly pointed out, this does not mean that all information has to be included in a single document, in multiple documents or as part of the final report documenting the DPIA process that has been followed. The form of presentation will depend on how the documentation can be organised in the most efficient way within the organisation, and it should be noted, as appropriate, that such an analysis has been carried out and that the controller of the possible processing is aware of it, supports it and is bound by it, from a regulatory point of view to its ultimate consequences.

In any case, the information to be found in the documentation is as follows:

Precise determination of the aims of the processing.	Final, specific, measurable, achievable and bounded.

Judgement of suitability

Defining the threshold of processing effectiveness	Establishing, in an objective, qualitative and evidence-based manner, what is the threshold of effectiveness that should be achieved to meet the aims of the processing.
Assessment of the effectiveness of the processing proposal	Assessing, in an objective, qualitative and evidence-based manner, the effectiveness of the processing as it has been planned, verifying whether it responds to the needs and to what extent.

Judgement of necessity

Determination of the relevance of the purposes of processing	Assessing that the purposes of processing are of sufficient importance to be addressed by high-risk processing.
Verification of the adequacy of processing operations	Verification that each of the specific processing operations is aimed at fulfilling the purposes of the processing in an objective and demonstrable manner.
Justification of the current processing setting	Assessing that there are no other processing, already underway or that could be considered, that address the stated purposes without incurring a high risk, even if some modification is necessary to meet the stated purposes.

Validity clauses provided for in the processing	Regarding its nature
	Regarding its scope
	Regarding its context
	Regarding its purposes

Judgement of proportionality in the strict sense

Identification of the degree of impact of the processing on rights and freedoms	Expressing, in detail, the limitations or intrusions to the rights and freedoms that the processing may entail for the data subject. This assessment is a prior task that has already been carried out in the determination of the risk factors and risk levels analysed previously, and its conclusions are set out at this point in the assessment.
Identification and description of compensatory measures	Detailing the controls put in place in the processing design to mitigate the impact.
Identifying the benefits of processing	Determining the purpose and evidenced benefits and advantages of processing for individual and collective data subjects. In other words, it is also necessary to consider the social benefit.
Confirmation of the existence of identity in the quality of information	It has to be assessed whether there is symmetry in the information analysed for the weighting judgement, i.e. whether the level of analysis in relation to the impact is equal to the level reached on the basis of the information provided regarding the benefits.
BHB (Benefit-Harm Balance) analysis	Assessing whether the benefits to the data subjets and society, previously determined, outweigh and justify the impact on rights and freedoms identified in point 1 of this proportionality test in the strict sense.

Table 49 Minimum information required in the assessment of the necessity and proportionality of processing.

XIV. DOCUMENTATION OBLIGATION

The DPIA is a process that needs to be documented[117], both in its findings and in its development process.

The WP248 Guidelines state that:

> *...a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.*

The rationale and the decision not to conduct the DPIA, made in the framework of risk management, should also be adequately documented. Failure to carry out documentation activities in relation to the active responsibility activities carried out, or failure to adequately and reasoned document the decisions of the controller, will prevent the controller from demonstrating compliance with its obligations and could lead to the initiation of an infringement procedure by the supervisory authority.

A. SUPERVISORY AUTHORITY ACCESS TO THE DPIA

All documentation relating to the DPIA must be available to the supervisory authority in two cases:

- Submission of a prior consultation (Article 36 GDPR).
- Request by the Supervisory Authority within the scope of the powers granted to it under Article 58 of the GDPR.

Therefore, there is no obligation to systematically submit all the DPIA carried out by the controller to the supervisory authority. However, where the conditions of obligation are met, failure to submit or incomplete submission of a DPIA to the supervisory authority could be considered as inaccurate information and therefore constitute an infringement.

With regard to the referral of the prior consultation to the Supervisory Authority, Article 39(e) of the GDPR provides that the DPO shall be the contact point for such management:

> *"(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter".*

B. DPIA TRANSPARENCY

There is no obligation to make public all documentation relating to an DPIA, nor is it even considered advisable. However, the WP248 Guidelines establishes that:

[117] As noted in this document, the word "document" does not imply the production of a single document, but to have recorded the actions, analyses and decisions of the DPIA, the criteria by which certain likelihood or impact values on data subjects are determined, the reasons why a certain measure leads to a reduction in likelihood or impact, the reasons why a certain risk assessment is considered acceptable, etc..

> *"Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA. ...*
>
> *In this context, the DPIA must be fully provided (Article 36(3)(e)).*

Therefore, the publication of those elements deriving from the conduct of a DPIA that could result in a transparency action and build data subject confidence is a best practice. In this case, the responsible person should avoid publishing unnecessary details that do not add value to such transparency or that would not be proportionate to new risks that their disclosure would create[118].

[118] For example, ICT security risks could arise if details of software used (versions, patches, etc.), network topology, organisational information facilitating or enabling social engineering attacks, details of security measures (firewalls, antivirus, etc.) are published. Security risks for individuals, trade secrets, contractual risks, etc. could also arise.

XV. SEEK THE VIEWS OF DATA SUBJECTS OR THEIR REPRESENTATIVES

One of the requirements of the DPIA when carrying out risk management (Article 35.9) is that “where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.”

This consultation is intended to make data subjects, or those presenting them, aware that the processing is high risk, detailing the risk factors, the potential impacts of data breaches and the intrusion on their rights and freedoms that this entails. In addition, the consultation should make data subjets aware that these risks are being taken for the sake of a greater good that compensates them, by identifying it precisely. In any case, the consultation should offer and collect from data subjets alternatives to meet the same objectives in a way that is less intrusive to their collective interests.

Therefore, the consultation of data subjects is intended to be an instrument of transparency and assessment of whether the appropriateness and necessity of the processing is justified and proportionality is appropriate. Consultation cannot be reduced to a satisfaction survey that only gives a picture of benefits, especially if those benefits are not directly related to the object of the processing and do not have an impact on the overall good.

XVI. PRIOR CONSULTATION OF THE SUPERVISORY AUTHORITY

Article 36 of the GDPR sets out the obligations to be fulfilled directly by the controller, and indirectly by the processor, where a DPIA has been carried out and, as a result of the DPIA, it has been concluded that the residual risk[119] of such processing could endanger the rights and freedoms of citizens.

Prior consultation is not an isolated action but must be integrated into the risk management strategy for rights and freedoms required by the GDPR. In this way, prior consultation is more than a simple referral of the DPIA to the supervisory authority. Prior consultation implies active collaboration, monitoring of the process and providing the Supervisory Authority with any additional information it may require during the consultation assessment process and from which actions by the controller could be derived.

However, it should be noted that, regardless of whether or not the Supervisory Authority must be consulted because of the level of residual risk, the obligations to keep a documentary record of the execution of the DPIA and of any updates of the assessment remain in place[120].

A. PURPOSE OF PRIOR CONSULTATION

The purpose of the prior consultation process is to submit to the supervisory authority a processing operation that is compliant with the GDPR, that is required or has been assessed as appropriate, or desirable, for a DPIA, but that involves a residual level of risk to the rights and freedoms of citizens that could be unacceptable.

It is not subject to prior consultation:

- Request the Supervisory Authority to assess the lawfulness of a processing operation.
- Request the Supervisory Authority to establish the legal basis for carrying out a processing operation.
- Transfer to the supervisory authority the controller's obligation to carry out the assessment of the proportionality and necessity of the processing.
- The systematic validation of any processing by the Supervisory Authority.
- Validation of the DPIA by the Supervisory Authority.
- The request to the Supervisory Authority to carry out the identification and assessment of the risks or the level of risk inherent in a given processing operation.
- Seek the advice of the Supervisory Authority for the conduct of the DPIA[121].
- Require the Supervisory Authority to indicate to the controller alternatives to the compliance requirements such as proportionality, necessity, duty of information, legal basis, conditions of consent, etc. considering

[119] Residual risk is not the risk that could originally arise from the processing, but is the risk that persists even after the implementation of the set of measures that the controller has deemed appropriate to address the identified risks

[120] WP248 Guidelines

[121] With this aim in mind, the supervisory authorities publish resources for help, in the case of the AEPD, which can be consulted at the following link
https://www.aepd.es/en/areas/innovation-and-technology

- such alternatives as possible technical and organisational measures to replace certain compliance requirements.
- Provide legal certainty for the responsible party[122].
- Request the Supervisory Authority to determine the appropriate technical and organisational security measures to ensure a level of security appropriate to the risk of the processing or request the agreement of the Supervisory Authority to the security measures put in place by the controller.
- Request the Supervisory Authority to determine the assumptions for international transfers.
- Nor is it the purpose of prior consultation to assess the possibility of derogating from the respect of a specific right or any other aspect which is not directly related to legitimate processing or which involves a high level of residual risk to rights and freedoms.

In general, it is not the purpose of the prior consultation to transfer to the Supervisory Authority any of the obligations that the GDPR and the LOPDGDD require of data controllers and processors.

B. THE OBLIGATION OF PRIOR CONSULTATION

The Supervisory Authority must be consulted on the appropriateness of a processing activity, and always before commencing it, where a data protection impact assessment shows that, in the absence of safeguards, security measures and mechanisms to mitigate the risks, such processing would result in a high risk to the rights and freedoms of natural persons, and the controller considers that the risk cannot be mitigated by reasonable means in terms of available technology and costs of implementation[123].

In addition, controllers must consult The Supervisory Authority whenever Member State law requires them to consult the supervisory authority or to seek its prior authorisation in relation to processing carried out by a controller in the exercise of a task carried out in the public interest, in particular processing in connection with social protection and public health (Article 36(5))[124.]

Therefore, prior consultation of the supervisory authority is not an obligation for any processing operation, not even for those processing operations where the controller has carried out a DPIA. Nor is the existence of a risk in the processing, understood as a risk to the rights and freedoms of citizens, a condition requiring prior consultation of The Supervisory Authority, just as the obligation or need to carry out a DPIA is not equivalent to the obligation to carry out prior consultation.

[122] The main purpose of the GDPR is to protect the rights and freedoms of data subjects whose personal data are processed. In addition, and secondly, the GDPR also provides a framework of legal certainty for the controller based on the risk approach and self-regulation. In this framework of active responsibility, legal certainty is guaranteed to the extent that the controller has adopted and effectively implemented the management of the processing operations it carries out and has the capacity to demonstrate this management process by means of the control measures it deems appropriate based on the particularities existing in each of its processing operations at any given time and taking into account the variables already mentioned and defined in the GDPR itself: nature, scope, context and purposes.

[123] Recital 94.

[124] WP248 Guidelines

In addition to the provisions of Article 36 of the GDPR, Article 28[125] of the LOPDGDD also establishes prior consultation among the general obligations of controllers and processors.

The processor should be aware that he/she is subject to certain obligations in relation to prior consultation. These are to be understood in the framework of the process of implementing such consultation, as set out in Article 36(2) when dealing with the role of The Supervisory Authority: *"...provide written advice to the controller and, where applicable to the processor..."*. Also, in Recital 95, it is described as part of the duties of the processor to assist the controller both during the conduct of the DPIA and during the prior consultation with the supervisory authority[126].

C. REQUIREMENTS FOR SUBMITTING A PRIOR CONSULTATION

There are a number of basic requirements to be fulfilled in order to submit a prior consultation to the Supervisory Authority. The following *checklist* identifies these requirements:

[125] Article 28. General obligations of the controller and the processor.
“Taking into account the elements listed in articles 24 and 25 of Regulation (EU) 2016/679, the controller and the processor shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the aforementioned regulation, this organic law, its developing regulations and the applicable sectoral legislation. In particular, they shall assess whether it is necessary to perform the data protection impact assessment and prior consultation referred to in section 3 of chapter IV of the aforementioned regulation.”

[126] Recital 95. The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

The controller submits the prior consultation	
If there is a DPO or an obligation to appoint one, he or she has advised on the data protection impact assessment and or is monitoring its implementation	
If there is a DPO or an obligation to appoint one, the DPO acts as a point of contact with the Supervisory Authority	
Prior consultation takes place prior to the implementation of the processing[127].	
The purposes of processing are objectively determined	
There is a systematic description of processing operations	
The assessment that the processing complies with the GDPR in terms of compliance with principles and rights has been carried out	
Risk management for data subjects' rights and freedoms is documented and carried out systematically	
The processing takes into account measures on the processing concept, governance and policies, data protection by design, data protection by default and security measures commensurate with managing the risk to the rights and freedoms of data subjects	
The analysis of the obligation to carry out the DPIA or, as the case may be, of the need to carry out the DPIA has been carried out	
The processing exceeds the necessity and proportionality analysis in relation to the purposes	
All of the above actions are formally documented	

Table 50 Minimum requirements for the submission of a prior consultation.

D. OBLIGATION OF PRIOR CONSULTATION IN THE CASE OF MISSIONS IN THE PUBLIC INTEREST

The second exception to the condition of high residual risk for prior consultation to be mandatory is set out in Article 36(5), which gives the possibility to each Member State to develop the obligation of prior consultation and prior authorisation for certain types of processing, specifically those relating to the exercise of a mission carried out in the public interest[128].

So far, no such obligations have been developed at national level.

E. ADDITIONAL TIME REQUIREMENTS FOR THE SUBMISSION OF PRIOR CONSULTATION

It has been described above that the GDPR established as the only time requirement for prior consultation that this must be carried out before the processing is carried out. The AEPD could, through circulars, establish additional conditions.

[127] See section "Exceptions to performing the DPIA prior to the start of processing activities"

[128] 36.5 "Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health".

F. HOW DOES PRIOR CONSULTATION MATERIALISE?

1. Documents

Article 36(3) sets out the documentation that must be submitted to the Supervisory Authority for prior consultation:

> *"3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:*
>
> *a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;*
>
> *b) the purposes and means of the intended processing;*
>
> *c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;*
>
> *d) where applicable, the contact details of the data protection officer;*
>
> *e) the data protection impact assessment provided for in Article 35; and*
>
> *f) any other information requested by the supervisory authority.*

The regulation makes it explicit that the data controller must attach to the prior consultation, in addition to the DPIA, additional information described in letters a), b), c) and d) of Article 35(3) of the GDPR; information that would make more sense if it were integrated into the documentation that forms part of the DPIA. This information is of a minimal nature and has to be filled in effectively.

2. Referral of prior consultation

Referrals to the AEPD for prior consultation relating to Article 36 of the GDPR must be made through its electronic office. This offers a specific section for the submission of prior consultations under the heading "Consultation prior to the start of high-risk processing operations (art. 36 GDPR)". This electronic procedure is aimed exclusively at data controllers for the submission of prior consultations and is not suitable for other types of consultations on other aspects of compliance with the GDPR.

In the case of having a DPO, this should be the point of contact with the Supervisory Authority[129].

G. RESPONSE OF THE SUPERVISORY AUTHORITY

1. Request for additional information by the Supervisory Authority

The possibility to request additional information directly from the controller is provided for in Article 36(2) and Article 36(3)(f) which states that the controller has to provide "*any other information requested by the supervisory authority*".

[129] 39.(e) to act as a contact point for the Supervisory Authority for matters relating to processing, including the prior consultation referred to in Article 36, and consult, as appropriate, on any other matters

In addition, when handling a prior consultation, the GDPR provides for the possibility to make use of the mutual assistance mechanism described in Article 61, both for advice in relation to the consultation and for resolving possible authorisations to carry out the processing[130].

Recourse to the mutual assistance mechanism is not regulated in the regulation except for the reference to compliance in order to apply the GDPR in a consistent manner. Thus, the request for mutual assistance is an action at the discretion of the supervisory authorities and allows for a suspension of the calculation of time limits. This mechanism is being effectively implemented, for example, in the framework of the meetings of the subgroups of the European Data Protection Board.

2. Deadline for a Reply

Deadlines for The Supervisory Authority to respond to a prior consultation are set at eight weeks, but could be extended to a total of 14 weeks. The extension of deadlines may be made "depending on the complexity of the processing", and the controller and, where appropriate, the processor must be informed of the reasons for such an extension. Therefore, the extension of the consultation period has to be reasoned on how problematic the analysis of the processing might be. The rationale for the complexity of the study could be established, for example, in terms of the technological innovation represented by the proposed processing.

However, these time limits may be suspended in cases where the Supervisory Authority has requested additional information for consultation purposes, which is necessary for its response, for as long as it takes to receive this information.

3. Extension of Advice

Article 57(1)(l) provides that it shall be the responsibility of each supervisory authority in its territory to give advice on the processing operation on which prior consultation is being carried out: "*57.1.l give advice on processing operations referred to in Article 36(2)*".

As a general rule and without prejudice to other considerations that may apply to the specific case of a request for prior consultation, the extent of the advice of the supervisory authority may include, inter alia, any of the following aspects:

- Point out to the controller that the processing could infringe the GDPR or the LOPDGDD.
- Determine whether the processing can be carried out under the risk conditions described by the controller.
- Report to the controller on the adequacy of the risk analysis provided in its DPIA.
- Inform the controller about the adequacy of the measures envisaged to mitigate or prevent risks to the rights and freedoms of natural persons posed by the processing.

[130] 1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

- Inform the controller about the correct analysis between the different alternatives for the implementation of the processing presented by the controller.
- Inform the controller about the correct assessment of necessity and proportionality.
- Carry out recommendations related to resources to assist the supervisory authorities.

The controller should not expect the response from the supervisory authority in the form of a report at the length that would result from an audit process. Nor is it the object of the response to provide the controller with a set of concrete solutions for processing that would correspond to the outcome of a consultancy process. Even less so, the purpose of the advice is to obtain a response to a new prior consultation by the controller in order for the Supervisory Authority to carry out the validation/review/approval/monitoring of the measures implemented in reaction to a previous consultation.

An audit should accurately state the state of the entity (or the processing) in relation to the subject matter of the audit[131]. Consultancy, on the other hand, offers specific solutions for the achievement of a specific objective set by the entity. Neither case constitutes the purpose of prior consultation, nor are they part of the powers of the Supervisory Authority.

Finally, this advice should not be understood in absolute terms in relation to the processing but in relation to those aspects that motivate the prior consultation and the information provided by the controller.

4. Exercise of the powers set out in Article 58 of the GDPR

In addition to advice, the second paragraph of Article 36 establishes that, in view of the information submitted by the data controller, the supervisory authority is empowered to exercise the powers set out in Article 58 of the GDPR.

This reference implies that, in case of prior consultation, the action of the Supervisory Authority is not limited to its advisory capacity, which is laid down in Article 58(3)(a), but can extend its action to the full range of powers laid down in Article 58, i.e. the powers of investigation laid down in Article 58(1) and the remedial powers of Article 58(2) which, among other possibilities, in relation to prior consultation, allow the Supervisory Authority to:

- Request additional information from the controller to that provided in the consultation.
- Conduct investigations of the controller in the form of audits which could include access to premises, equipment, data and information necessary for the exercise of the functions of the Supervisory Authority.
- In the event that the processing is being carried out, notify and fine the controller, inter alia, when:
    - the mandatory DPIA has not been carried out, although there is a legal obligation to do so (35 GDPR, paragraphs 1, 2, 3 and 4) [132],

[131] The audit process that can be carried out by the Supervisory Authority is defined, in another context, in Section 2 "Investigatory powers and preventive audit plans" of the LOPDGDD.

[132] As stated in the Guidelines on the Data Protection Impact Assessment (DPA) and for determining whether the processing is 'likely to involve a high risk' for the purposes of Regulation (EU) 2016/679, non-compliance with the requirements of the DPIA may lead to the imposition of fines by the competent supervisory authority, as determined in Title IX of the LOPDGDD (Articles 73.t, 73.u and 74.o).

  - the DPIA has been carried out incorrectly (Article 35 GDPR paragraphs 2, 7, 8, and 9),
  - and, where applicable, inaccurate information was provided to the Supervisory Authority in the prior consultation.
- Require the controller or processor to carry out the necessary modifications to the processing in order to bring the processing in line with the provisions of the GDPR and the LOPDGDD.
- Prohibit or impose temporary or definitive limitations on processing.

H. TRANSPARENCY AND CONFIDENTIALITY OF PRIOR CONSULTATIONS

Prior consultations, as we have seen above, should include detailed information on the implementation of the processing and even technical and organisational aspects of the controller entity. These aspects can be of great importance as they reflect issues as relevant to the entity as its policies, values, procedures, strengths, weaknesses, corporate security measures and business purposes that are crucial to understand the scope of the processing and its context.

1. Transparency

With regard to determining whether the information submitted to the Supervisory Authority in the framework of a prior consultation, provided for in article 36 of the GDPR, is covered by Law 19/2013 on Transparency, Access to Public Information and Good Governance (LTAPIGG), it should be noted that, on the one hand, such information would be excluded from the scope of active disclosure, as it would not fall under any of the cases contemplated in articles 7 and 8 of the LTAPIGG.

On the other hand, such information would not in principle be subject to the right of access to public information either. Although it is public information, it would be affected by the limits to the right of access set out in Article 14, to the extent that its disclosure would prejudice (i) the prevention, investigation and sanctioning of criminal, administrative or disciplinary offences, (ii) administrative functions of surveillance, inspection and control, (iii) economic and commercial interests, (iv) economic and monetary policy, or (v) professional secrecy and intellectual and industrial property.

2. Confidentiality

With regard to the confidentiality of information submitted to the Supervisory Authority, the GDPR establishes in Article 54(2) that confidential information obtained in the performance of its duties is protected by the duty of secrecy to which the members and personnel of the Supervisory Authority are subject[133].

Similarly, the WP248 Guidelines stipulate that the Supervisory Authority shall not compromise trade secrets or disclose security vulnerabilities,

[133] Article 54. Rules on the establishment of the supervisory authority
"2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation".

which in turn obliges not only the duty of secrecy of its personnel, but also the implementation of the necessary security measures to guarantee the achievement of this objective[134].

I. RELATED LEGISLATION

The obligation to carry out a prior consultation regarding the risks arising from the processing of personal data is also present in other legislation such as, for example, in Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, which transposes Directive (EU) 2016/680. Article 35 establishes the conditions for the mandatory conduct of the DPIA and Article 36 extends the obligation of prior consultation to any of the following circumstances:

a) Where the data protection impact assessment indicates that the processing would result in a high level of risk, in the absence of measures taken by the controller to mitigate the risk or potential damage.

b) Where the type of processing is likely to result in a high level of risk to the rights and freedoms of data subjects, in particular where new technologies, mechanisms or procedures are used.

In turn, in the proposal for a Regulation of the European Parliament and of the Council on privacy and the protection of personal data in the electronic communications sector and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications), with the necessary caution that this is a proposal subject to thorough revision at the time of writing this text, Article 6 on "Authorised processing of electronic communications data", refers to the fact that providers of electronic communications services may only process electronic communications content where all end-users concerned have given their consent to the processing of their electronic communications content for one or more specific purposes that cannot be achieved by processing anonymised information, and the provider has consulted the Supervisory Authority, with Article 36(2) and (3) of Regulation (EU) 2016/679 being applicable to prior consultation.

[134] "The supervisory authority may provide its advice and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents".

XVII. CONCLUSIONS

As mentioned in the introduction, risk management is an exercise of reflection to be carried out before engaging in a personal data processing activity. Its purpose is to identify and be able to anticipate possible adverse or unintended effects that the processing might have on data subjects. Risk management must enable the controller to take the necessary decisions and actions to ensure that the processing complies with the requirements of the GDPR and the LOPDGDD, guaranteeing and being able to demonstrate the protection of data subjects' rights.

Risk management is a task that confronts the expectations and illusions of the controller with the reality of the consequences of the actual implementation of the processing for the data subjects. It also confronts the short-term purposes of the controller with a long-term view of the consequences that processing operations may have on data subjects. It also requires a critical analysis of the relationship between processing and the context.

The risk management required by the GDPR is that which is specifically aimed at protecting the rights and freedoms of data subjects, and should not be confused with other risk orientations, such as compliance risk management. In turn, risk management for rights and freedoms extends beyond security risk management alone.

The proper performance of this task requires the controller to do more than produce documents or use decision-support tools. Risk management, which requires study, analysis, action and accountability, as well as continuous and ongoing monitoring. Risk management is therefore a process and, as such, it has to be effective (achieving its objectives) and efficient (carried out with the minimum cost and use of resources).

As a basic tool for the implementation of accountability, risk management for rights and freedoms must be included and form an indivisible part of the organisation's management policies. Therefore, risk management for rights and freedoms is a task that must be performed "by default" when personal data are being processed.

Risk management and Data Protection Impact Assessment are closely linked processes. DPIA is a specificity within risk management. Therefore, the DPIA cannot exist without being part of risk management for rights and freedoms, extending it with a number of additional requirements. While risk management is mandatory for all processing, the specific obligations set out for the DPIA are mandatory only for high-risk processing.

The obligation to carry out an DPIA, established in the GDPR and its implementation, is a declaration on minimum requirements. In other words, DPIA may be advisable or necessary in other cases, regardless of whether it is mandatory for specific cases. Its use may sometimes be advisable, as a tool to "ensure and be able to demonstrate” [135] compliance with the GDPR. In any case, irrespective of guidelines or obligation lists, risk management including the safeguards of an DPIA has to be performed "Where it is likely that a type of processing, in particular if it uses new technologies, by its nature, scope, context or purposes, entails a high risk to the rights and freedoms of natural persons” [136.]

[136] Article 35.1 of GDPR