Checklist for determining the FORMAL adequacy of an DPIA AND THE SUBMISSION OF PRIOR CONSULTATION

# Introduction

The Data Protection Impact Assessment (DPIA/DPIA) is a process which is part of the risk management of rights and freedoms to be carried out by the controller. To facilitate the task of addressing risk management for rights and freedoms with the level of detail required by an EIPD, the AEPD has published the guide on [Risk Management and Impact Assessment in Personal Data Processing](https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf) (hereinafter, "the Guide"). This Checklist is intended to help those responsible to quickly identify and determine whether the DPIA process and documentation contains all the minimum formal elements expected of DPIA. In particular, compliance with this checklist will allow you to formally ensure that the request for prior consultation that could be made in relation to the EIPD complies with the requirements to be considered as such.

Article 35(7) of [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data](https://www.aepd.es/es/documento/reglamento-ue-2016-679-consolidado.pdf) (GDPR) sets out the minimum content of a DPIA. In turn, the "[Guidelines on Data Protection Impact Assessment (DPA) and for determining whether processing is 'likely to involve a high risk' for the purposes of Regulation (EU) 2016/679](https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf)" of the European Data Protection Board (hereinafter "Guidelines") interpret that a DPIA has to be carried out with minimum quality requirements.

According to the above-mentioned Guidelines, the implementation of a DPIA is not merely a formal compliance requirement, but *"a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons arising from the processing of personal data by evaluating them and identifying measures to address them", a* process that applies to the entire life cycle of the processing and not only to a specific point in time of the processing[[1]](#footnote-1).

The outcome of such a process should be adequately documented. This documentation should include at least the systematic description of the processing operations, the assessment of necessity and proportionality of the processing operations, an assessment of the risks to the rights and freedoms of data subjects and the measures to address those risks (Article 35(7) GDPR) which should include the measures required by Article 32 of the GDPR.

With regard to the minimum required content of a DPIA, in Annex 2 "Criteria for an acceptable DPIA" of the Guidelines, the Article 29 working group proposed a set of minimum elements that had to be included in the DPIA documentation. These elements were set out in a basic checklist that controllers could use to self-assess their own DPIA. The experience acquired by the AEPD since the effective application of the GDPR allows for a more precise definition of the elements described therein. These elements will be those that the Control Authority will require in order to determine that a DPIA complies with the minimum formal requirements, and which are already included in the AEPD Instruction 1/2021.

On the other hand, with regard to the advisory function on processing operations contemplated in Article 36.2 of the GDPR, Chapter IV of [Instruction 1/2021, of 2 November, of the Spanish Data Protection Agency, establishing guidelines regarding the advisory function of the Agency, in accordance with Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data](https://www.boe.es/boe/dias/2021/11/05/pdfs/BOE-A-2021-18134.pdf), and the [Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights](https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673) (LOPDGDD) require the controller, in relation to its obligations regarding the processing of personal data, minimum requirements of which further information can be found in the guide on [Risk Management and Impact Assessment in Personal Data Processing](https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf%22%20%5Ct%20%22https%3A//www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf).

In the case of prior consultation, Instruction 1/2021 establishes that the data controller must contemplate what is indicated by the AEPD in its guidelines and recommendations; consequently, the data controller must include this completed checklist to the supervisory authority in order to include the minimum content required and provide its consultation with greater precision and accuracy.

The GDPR establishes and typifies infringements in the case of absence or inadequacy of the development of the DPA when it is necessary to carry it out. Specifically, the GDPR establishes in Article 83.4 that infringements of Articles 35 "Data Protection Impact Assessment" and 36 "Prior Consultation" shall be punishable by administrative fines of up to EUR 10,000,000 or, in the case of a company, an amount equivalent to up to 2% of the total annual aggregate turnover of the preceding financial year, whichever is greater.

The LOPDGDD, for the purposes of limitations, establishes as serious infringements:

* Failure to carry out a DPIA where one is required:
	+ 73.t The processing of personal data without having carried out an assessment of the impact of the processing operations on the protection of personal data in the cases in which this is required.
* A specific infringement for the case of incorrect performance of the DPIA, which is the non-participation of the DPO when appointed:
	+ 73.w Fail to enable the effective participation of the data protection officer in all matters relating to the protection of personal data, to support him/her or to interfere in the performance of his/her duties.
* Failure to consult with the control authority on the DPIA when required (which is not always the case):
	+ 73.u Processing personal data without prior consultation with the data protection authority in cases where such consultation is required under Article 36 of Regulation (EU) 2016/679 or where the law provides for an obligation to carry out such consultation.

The LOPDGDD establishes as minor infringements:

* Providing inaccurate information to the supervisory authority in the framework of a prior consultation. It should be recalled that, in the case of prior consultation, all information on the DPIA must be provided (Art. 36.3.e):
	+ 74.o Providing inaccurate information to the Data Protection Authority, in cases where the controller is required to submit a prior consultation to the Data Protection Authority in accordance with Article 36 of Regulation (EU) 2016/679.

Before going on to review the checklist, it is necessary to take into account some previous considerations, which were already established in the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf):

* As a precondition for risk management, the processing must be compliant with the GDPR. The compliance assessment should address each of the principles required by the GDPR and not only the requirement to carry out the DPIA.
* An impact assessment, as part of risk management for rights and freedoms, is not a compliance risk analysis. Nor is it reduced to a compliance checklist, such as the AEPD Compliance Checklist.
* In no case can any defects that may be identified in relation to the mandatory principles be mitigated or eliminated by risk control measures. Risk management cannot be used as an alternative to compliance with the provisions of data protection regulations.

This checklist is intended to serve as a checklist on the risk management process, the DPIA and the integrity of the DPIA documentation. This document is not intended to reduce the proactive accountability required by the GDPR to a checklist. In this regard, it is important to emphasise that completing this checklist does not amount to conducting a DPIA, nor does it constitute the DPIA report. In other words, the checklist is not a risk management tool and its preparation does not replace the documentation of a DPIA.

The usefulness of this checklist is that it is a tool to check, and if necessary declare, that the minimum formal actions required to carry out a DPIA have been carried out. The guide on [Risk Management and Impact Assessment in Personal Data Processing](https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf%22%20%5Ct%20%22https%3A//www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf) sets out the details of the tasks and minimum contents that must be taken into account in the execution and documentation of the DPIA. Failure to respond to these contents may mean that the DPIA is not correct or that the information provided is inaccurate.

To complete the checklist, it is necessary to go through each of the rows and update the value of the "CHECK" column, which is a selection field (marked by default as "NO"), when the described action has been performed and/or adequately examined and/or documented in the framework of the carried out DPIA. The comments column should then be updated with any appropriate observations/conclusions that refer to, and/or redirect to, the documentation of the DPIA. It means, the comments column has not the aim to include the information that should be detailed in the DPIA documentation. It would not be appropriate, for example, in the case of the check in 9.9, to include in the “Comments” column the list of privacy by design actions and measures and the criteria for their selection. Such information should be part of the DPIA documentation.

Below is the checklist of the formal content to be included in the DPIA documentation in order to determine its adequacy, in particular for submission in the framework of a prior consultation as set out in Article 36 GDPR.

# Checklist

## General requirements for prior consultation (Fifth.1-2 of Instruction 1/2021)

If prior consultation is deemed necessary, the following requirements and certain additional information outlined below should be taken into account:

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 1.1 The high risk level of data processing cannot be mitigated by appropriate measures and the need for Prior Consultation has been assessed (Art. 36, Recital 84). | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation, a brief description of the reasons why the residual risk is not acceptable or why there are no measures to mitigate and/or eliminate the residual risk was provided. |
| 1.2 Prior consultation and the DPIA are carried out prior to the start of processing. | NOYES, AND IT IS DEMONSTRATED | If the answer is “no”, check the next item on the checklist. |
| 1.3 If the prior consultation and the DPIA are carried out after the processing has started, there is an objectively motivated justification. | NO, THE EIPD IS PRIOR TO PROCESSINGYES, THE EIPD IS AFTER THE START OF PROCESSING AND JUSTIFIED | If so, justification shall be provided that the processing has undergone changes in its nature, scope, context, purposes or that a significant variation in relation to the risks of processing has been identified, in which case such variation shall be justified in sufficient detail. |

## Requirements on the DPO (Fifth paragraph.3 of Instruction 1/2021 and art. 35.2 and 39.1.c GDPR).

Regarding the role of the DPO in the elaboration of the DPIA and the Prior Consultation:

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 2.1 If there is an obligation to have a DPO, the DPO is appointed and the Supervisory Authority has been notified (art. 36.3.d and 37 GDPR and art. 34 LOPDGDD). | NOYES, AND IT IS DEMONSTRATED | Failure to comply with these requirements could be an infringement in itself, regardless of the DPIA conducted. |
| 2.2 If a DPO exists, the data controller has sought the advice of the DPO upon request (art. 35.2 and 39.1.c GDPR). | NOYES, AND IT IS DEMONSTRATED | The controller shall seek the advice of the DPO, if appointed, when carrying out the Data Protection Impact Assessment. |
| 2.3 If there is a DPO, the DPO supervises the implementation of the DPIA (art. 39.1.c GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPO will supervise the implementation and execution of the DPIA as well as the implementation and monitoring of the DPIA throughout the life cycle of the processing. |

## Identification of the processing and those involved (art. 35.7.a GDPR, Fifth.5.a, b, e of Instruction 1/2021).

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 3.1 The DPIA documentation identifies the processing with a name and, where appropriate, a version. | NOYES, AND IT IS DEMONSTRATED | The processes of an entity and the development projects of systems, products and services may require one or more processing of personal data. Each processing of personal data shall be individualised by the controller.The name of the processing operation may be any means of identification internal to the entity and which allows traceability with the Register of Processing Activities (RPA) and other management elements internal to the entity.The identification of the version should make it possible to differentiate between different possible configurations or implementations of the processing throughout its life cycle (traceability). |
| 3.2 The DPIA includes the date and signature of the data controller, as well as his/her contact details and, where applicable, the contact details, date and signature of the DPO (Chapter IV GDPR, art. 28 LOPDGDD) as well as traceability information on who has been involved in its preparation/updating. | NOYES, AND IT IS DEMONSTRATED | The controller has the obligation to draw up the DPIA (art. 35.1 GDPR), accrediting traceability and diligence in the selection of those who have been involved in its preparation (proactive responsibility). |
| 3.3 The controllers, joint controllers, processors and other parties involved in the processing are unambiguously identified (Arts. 26, 27 and 28 GDPR). | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation, the parties involved in the processing are unambiguously identified, including their contact details in relation to the identified processing. |
| 3.4 The obligations and tasks of controllers, joint controllers, processors and other parties involved in the processing (Articles 26, 27, 28, 36.3.a GDPR) are unambiguously set out. | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation, each controller, co-responsible, processor or sub-processor has detailed responsibilities, functions and roles in the corresponding instrument or legal link with the controller or processor. |
| 3.5 The description incorporates the inclusion, or potential inclusion, of the processing in the Register of Processing Activities (art. 30 GDPR, art. 31 LOPDGDD). | NOYES, AND IT IS DEMONSTRATED | The RPA should be understood as part of the basic and initial processing description and as a basic asset in the risk management or processing management approach. |
| 3.6 In the case of entities listed in Art. 77.1 LOPDGDD, the description incorporates the inclusion or potential inclusion of the processing in the inventory of processing activities (Art. 31.2 LOPDGDD). | NOYES, AND IT IS DEMONSTRATED | The entities listed in Article 77(1) must draw up the inventory referred to in Article 31(2) LOPDGDD prior to the implementation of the processing, which forms part of the description of the processing and constitutes a further way of addressing the principle of transparency. |

## Updating of a prior consultation (Fifth.5.c of Instruction 1/2021)

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 4.1 If a prior consultation on the same processing operation has been submitted in advance, the changes made to the nature, context, scope, purposes, risks and safeguards of the processing operation as a whole must be detailed. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation needs to include the history of changes and modifications to the processing in relation to its nature, context, intended scope, purposes, risks and safeguards implemented. |
| 4.2 If there are prior consultations with a Supervisory Authority, an explicit reference to the response(s) of the Supervisory Authority(ies) is included. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation should disclose the safeguards implemented in the processing to mitigate or alleviate the identified risks based on the responses that a supervisory authority would have given in relation to the processing of personal data covered by the DPIA. |

## Context of the processing and the DPIA (art. 35.7.a GDPR, Fifth.5.d of Instruction 1/2021)

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 5.1 A description of the internal context of the organisation in which the processing takes place is included. | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation there is a brief description of the organisation's structure, functions and competencies, adopted policies, norms and standards, organisational maturity objectives and in general the organisation's culture. |
| 5.2 Description of the context external to the organisation in which the processing takes place. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation includes a description of the scope and extent of the processing, the regulatory and social environment relevant to the processing, personal data breaches in similar processing or entities and possible side effects (those not related to the purpose of the processing). |
| 5.3 Data protection policies applicable to the processing have been identified (art. 24.2 GDPR). | NOYES, AND IT IS DEMONSTRATED | If the controller has data protection policies in place within the organisation that apply to the processing under scrutiny, the DPIA should include these policies and indicate how they apply to the intended processing. |

## The processing complies with the requirements of the GDPR (art. 24 GDPR, Fifth.5.f Instruction 1/2021).

Regulatory compliance is not the subject of analysis of a DPIA, but rather the prerequisite for its preparation, in particular, the absence of a legal basis would constitute a requirement that cannot be remedied by other compliance measures.

Without prejudice to a possible more exhaustive analysis of compliance that includes a greater detail of the regulatory compliance requirements, such as the [list of regulatory compliance](https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf) published by the AEPD, some of the most relevant aspects whose absence, since the entry into force of the GDPR, have been observed in the reports and documents that have been sent to this Agency and which, inexorably, must be taken into account as elements of mandatory compliance, are indicated below.

Remember that the process of the DPIA and the analysis of risks to rights and freedoms must be carried out once compliance with the regulatory requirements of the GDPR and the LOPDGDD is guaranteed. Under no circumstances should the DPIA be understood as a mere verification of the regulatory compliance requirements or a closed list of security measures, nor should the DPIA be understood as a way of addressing compliance by replacing the compliance requirements with alternative elements, in particular, technical, organisational or security measures.

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 6.1 The purpose(s) exist and are described (Arts. 5.1.b, 5.1.c and 36.3.b GDPR and section III.A of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation defines and justifies that the goals are ultimate, specific, achievable, measurable and limited.This description must be complete, also stating further, intended or collateral purposes, transfers of data and must be carried out in accordance with the principle of fairness in Article 5(1) of the GDPR. |
| 6.2 An analysis of the legal bases for processing (Art. 6 GDPR) has been carried out. | NOYES, AND IT IS DEMONSTRATED | It must be carried out and described in the DPIA documentation and for each of the purposes of the processing in relation to its possible legal bases. |
| 6.3 The analysis of the legal bases has been carried out in relation to each of the purposes of the processing, including secondary or further purposes. | NOYES, AND IT IS DEMONSTRATED | The processing operations may incorporate different purposes, and in that case, the legal bases for each of them must be detailed separately in the DPIA documentation. |
| 6.4 If the lawfulness of the processing is based on consent (Article 6(1)(a) of the GDPR), the conditions set out in Article 7 and Recitals 32, 42 and 43 of the GDPR have been analysed. | NOYES, AND IT IS DEMONSTRATED | The analysis of the conditions of free, specific and informed consent that guarantee the absence of asymmetries and the full freedom and knowledge of the data subject at the time of giving consent must be included in the documentation of the DPIA. |
| 6.5 If the lawfulness of the processing is based on legitimate interest (Art. 6.1.f GDPR), a balancing of rights has been carried out, in particular when it concerns minors or persons at risk of social exclusion or other circumstances that could lead to discrimination against data subjects. | NOYES, AND IT IS DEMONSTRATED | If the lawfulness of the processing is based on legitimate interest, the legitimate interest must be identified, which must be at least as broad as the purpose of the processing and be present and effective at the date of processing, the necessity of processing the personal data for the fulfilment of that interest must be justified, and the required balancing of interests against the rights and freedoms of data subjects, including the rights to data protection, must be carried out. |
| 6.6 If the lawfulness of processing is based on the fact that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the enabling regulation shall be specified (Art. 6.3 GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation shall identify the rule, the article and the text that specifically defines the purpose-of-processing authorisation, as well as the specific provisions for adapting the application of the rule to the GDPR.The regulatory analysis must be complete, without providing a partial view of the regulation of only those elements that support the vision of the decision-maker.This legislation will be incorporated into the analysis of the context of the DPIA during the life cycle of the processing. |
| 6.7 If the lawfulness of processing is based on the fact that the processing is necessary for compliance with a legal obligation applicable to the controller, the enabling regulation shall be specified (art. 6.3 GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation shall identify the rule, the article and the text that specifically defines the purpose-of-processing authorisation, as well as the specific provisions for adapting the application of the rule to the GDPR.The regulatory analysis must be complete, without offering a partial view of the regulations, only those elements that serve to support the vision of the decision-maker.This legislation will be incorporated into the analysis of the context of the DPIA during the life cycle of the processing. |
| 6.8 Prior to determining the legitimacy of the processing, in the event of processing special categories of data, determine the grounds for lifting the prohibition on processing such special categories of data (art. 9 GDPR) and whether it is compatible with the provisions of art. 9 LOPDGDD. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation specifically and unambiguously determines that the conditions for lifting the prohibition are met, irrespective of the basis on which the processing is lawful.If the lifting of the prohibition is based on a regulation, the regulation, the article and the text that specifically defines the purpose-of-processing authorisation, as well as the specific provisions for adapting the application of the rule to the GDPR shall be identified.The regulatory analysis must be complete, without providing a partial view of the regulation of only those elements that support the vision of the decision-maker.This legislation will be incorporated into the analysis of the context of the DPIA during the life cycle of the processing. |
| 6.9 If the lifting of the prohibition on processing special categories of data is based on consent, the conditions set out in Article 7 and Recitals 32, 42 and 43 GDPR have been analysed. | NOYES, AND IT IS DEMONSTRATED | If the lifting of the prohibition on the processing of special categories of data is based on consent, the analysis of the conditions of consent required by Article 7 of the GDPR and recitals 32, 42 and 43 must be carried out. The relevant analysis must be carried out in order to ensure and demonstrate that the consent is specific, unambiguous, free and informed, demonstrating, for example, the absence of asymmetries and the full freedom and knowledge of the data subject at the time of giving consent |
| 6.10 There is clear identification of the data controller (art. 36.3.a GDPR). | NOYES, AND IT IS DEMONSTRATED | The identification of the controller(s) shall be included in the documentation of the DPIA, in case of co-responsibility.The purposes and means, if any, determined by each of the responsible parties should be indicated. |
| 6.11 Where applicable, there is an agreement or legal act between the joint controllers involved or third parties involved in the processing (Arts. 26, 27 and 28 GDPR). | NOYES, AND IT IS DEMONSTRATED | The documentation of the DPIA shall include details of the legal agreement between the co-responsible parties involved or third parties involved with identification of respective responsibilities, in particular as regards the exercise of rights and reporting obligations.Where applicable, the rule covering the co-responsibility or involvement of the third parties involved in the processing. |
| 6.12 Processors and the contracts or other legal acts linking them to the controller or co-responsible parties are identified (Art. 28 GDPR). | NOYES, AND IT IS DEMONSTRATED | The identification of the processor(s) shall be taken into account in relation to each of the purposes and processing operations that may be carried out during the life-cycle of the data.This should include details of the legal link between controllers and processors, as well as between the other entities that may be involved in the processing, and an explanation of the care taken in the selection of processors or those involved in the processing. |
| 6.13 Adequate legal safeguards are in place to ensure that controllers are consulted by processors before engaging sub-processors or third parties involved in the processing (Arts. 28.2 and 36.3.a GDPR). | NOYES, AND IT IS DEMONSTRATED | The controller-processor legal link shall incorporate the obligation of the processor to consult with the controller before delegating the hiring of sub-processors or the involvement in the processing of any other involved third party. |
| 6.14 Measures have been established that allow the responsible party to guarantee and demonstrate compliance with the provisions of the GDPR and LOPDGDD (Arts. 5.2, 24 to 36, and Recital 90 GDPR, WP248). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation shall include information demonstrating the implementation of proactive accountability measures and safeguards (e.g. governance, nature of implementation, policies, data protection by design, data protection by default, security measures and personal data breach management). |
| 6.15 The legal link established between controllers, processors and sub-controllers specifies and defines the proactive liability measures and guarantees to be implemented by the processor and the monitoring mechanisms (Arts. 35.7.d and 36.3.a GDPR). | NOYES, AND IT IS DEMONSTRATED | If there are processors and sub-processors, the legal link between the controller and a processor should reflect the obligations of the processor and any sub-processors in relation to the application of the proactive accountability measures and safeguards (governance, nature of implementation, policies, data protection by design, by default, security measures and personal data breach management, among others) identified by the controller. |
| 6.16 The obligations to inform data subjects (Arts. 12, 13 and 14 GDPR) are complied with. | NOYES, AND IT IS DEMONSTRATED | The EPIA documentation shall identify the procedures used to address the obligation to inform data subjects, including the transparency mechanisms and the policies for informing data subjects that may be applicable in each case or justify the exemption from the obligation to inform.For more information, you can use the AEPD's [Guide for compliance with the duty to inform.](https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf) |
| 6.17 Procedures are in place to guarantee the rights of data subjects: access, rectification, erasure, restriction of processing, portability, objection and those corresponding to possible automated individual decisions (Arts. 15-20 GDPR). | NOYES, AND IT IS DEMONSTRATED | The existence of policies and procedures to address data subjects' rights should be reflected in the documentation of the DPIA, if data subjects are informed of them and it is possible to demonstrate that they are implemented.In turn, it is also necessary that the procedures are known by all persons involved in the processing, identifying the information and training policies implemented for this purpose. |
| 6.18 The processes, products and services associated with the processing and the cases in which data subjects may be offered the right to portability (Arts. 15 and 20 GDPR) have been identified. | NOYES, AND IT IS DEMONSTRATED | It is recommended to implement a data protection policy in relation to the rights of data subjects (art. 24 GDPR) identifying the need to inform the data subject in relation to the right to portability in cases where there is the possibility of applying this right depending on each of the products, processes and services for which the processing will be used.This information on portability should be provided to the data subject both at the beginning and at the end of the processing and throughout the life cycle of the processing, e.g. where the data subject requests to unsubscribe from a service and the right of portability is applicable, clear information on the possibility of exercising the right of portability should be provided prior to the erasure of the data subject's data relating to the service. |
| 6.19 The data used are adequate, relevant and limited to what is necessary to address the identified purposes (Art 5.1.c, Art. 25.2 GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation should include, for each data, grouping of data, and category of data, a necessity analysis of the data in relation to the purpose of processing to demonstrate that only the data minimally necessary for the purpose(s) of processing are being used. |
| 6.20 Time limits are established for the limitation of processing operations in relation to data (art. 5.1.e GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation details the retention periods, locking procedures and destruction or erasure mechanisms used at the end of the retention period. |
| 6.21 Treatment time limits have been established (section XIII.C.1 of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | In relation to the analysis of the necessity of the processing, expiration clauses should be established for the processing and a periodic review of the necessity of the processing should be carried out so that in case of the disappearance of the necessity for which the processing is intended, a procedure for terminating the processing activity should be established. |
| 6.22 In the case of international transfers, compliance with the necessary safeguards set out in Chapter V of the GDPR is documented. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation shall reflect the details regarding the safeguards required by the GDPR for the implementation of an international data transfer, including in those cases where the processor may carry out an international transfer, in which case, those safeguards shall be reflected in the legal link between the controller and the processor. |
| 6.23 Compliance with the approved codes of conduct (Article 35, paragraph 8) to which the officer has adhered is managed. | NOYES, AND IT IS DEMONSTRATED | In case the controller has adhered to a code of conduct, the DPIA documentation identifies the procedures to demonstrate that the processing complies with the provisions of such code. |

## There is a systematic description of the processing (art. 35.7.a GDPR, Fifth.5.g of Instruction 1/2021).

A description of the processing, including sufficient information to draw objective conclusions about the processing, needs to be incorporated into the DPIA documentation.

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 7.1 The nature, scope and context of the processing are fully described (Recital 90 GDPR and Section V.A of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | The following should be taken into account: applicable sector-specific rules, social aspects, socio-economic characteristics of data subjects, typology of data, typology of data subjects taking into account their possible situations of vulnerability, etc.It is recommended to use a high-level diagram indicating the relationship of the treatment to the business processes to which it is intended to respond (products, processes and services). |
| 7.2 A structured treatment analysis is included. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation, for each processing step, details the different processing operations that may be part of a processing operation, and the relationship between them. In particular, it details those that are of interest from a data protection point of view. |
| 7.3 A description of the data life cycle is included. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation, for each of the processing steps, details the data processed (direct identifiers, indirect identifiers, inferred data, origin and sources of the data, etc.).It should also detail the periods of limitation of use of the data in relation to the purpose pursued, the rules obliging the establishment of limitation periods that may be applicable to the processing, data blocking procedures if any, and/or measures restricting access to information in relation to such limitations.Please note that not all data necessary for processing may be subject to the same limitations.If the end of the data's life cycle involves its total or partial destruction, the destruction, erasure or blocking procedure used should be added, which should be understood as one of the processing operations carried out. |
| 7.4 A description of the assets involved in the processing and the vulnerabilities and threats to which they are exposed is included in order to determine the set of security measures necessary for the protection of the rights and freedoms of data subjects (Art. 32 and Recital 87 GDPR, section V.D of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation, for each step of the processing in accordance with the data life cycle, the technological means and aspects related to the processing of personal data (hardware, software, networks, persons, media -paper, electronic, etc. - or transmission channels, and all those necessary to carry out the processing) are identified.In turn, the technical and organisational measures related to the processing (persons, facilities, non-technical procedures...) are identified, taking into account the nature, scope, context and purposes of the processing in such a way as to ensure the confidentiality, integrity and resilience of the systems and services on which the processing is carried out. |
| 7.5 The use cases of the processing are described (section V.E of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | In the event that the functionalities of the processing may vary depending on the configuration of the processing or other factors, the different use cases should be identified and their differences marked. The identification of use cases, with examples, has been discussed in the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf) (section V.E). |
| 7.6 The default privacy measures are identified and documented and their implementation is planned (art. 25.2 GDPR). | NOYES, AND IT IS DEMONSTRATED | It is recommended to consult the following resources for help:* [Default Data Protection Guide](https://www.aepd.es/media/guias/guia-proteccion-datos-por-defecto.pdf)
* [Data protection by default: List of measures](https://www.aepd.es/media/guias/PDpD-listado-medidas.xlsx%22%20%5Ct%20%22https%3A//www.aepd.es/media/guias/PDpD-listado-medidas.xlsx)
 |
| 7.7 Details of data transfers are included (Chapter V of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation includes a description of the transfers in relation to the purposes, to the life cycle of the processing, to the life cycle of the data and of the processing operations. All such recipients should be listed together with the functional description in which such transfers are carried out for each recipient.Link it to the legal bases legitimising such transfers described above. |
| 7.8 The certification mechanisms, seals and data protection marks that apply to the processing are described (Arts. 42 and 43 GDPR). | NOYES, AND IT IS DEMONSTRATED | In the event that there are data protection certifications, seals and marks applicable to the processing, the scope of such certifications, seals and marks must be detailed, along with the documentation accrediting that they are in force and detailing the procedures that make it possible to demonstrate that the processing complies with the requirements of the data protection certification, seals and marks. |
| 7.9 The codes of conduct on which the processing is based are identified (Art. 35.8 GDPR). | NOYES, AND IT IS DEMONSTRATED | Where applicable, codes of conduct to which the controller has adhered in relation to the intended processing should be included. |

## There is an analysis of obligation and an analysis of necessity to carry out the DPIA (art. 35 GDPR, wp248, others, Fifth.5.h of Instruction 1/2021).

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 8.1 The processing is covered by the list in Art. 35.3 GDPR, the Guidelines document (WP248), other Guidelines or opinions of the European Data Protection Committee, or the conditions in the lists in Art. 35.4 GDPR which imply the obligation to carry out the DPIA. | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation determines the criteria according to which the controller considers that the controller is obliged to carry out a DPIA.Include the regulation and the section detailing the obligation to carry out the PIA for the particular processing.If applicable, include the specific/sectoral regulations that imply the obligation to carry out the PFIA. |
| 8.2 In accordance with art. 35.1 GDPR, and with the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf), there are risk factors identified by the data controller that make the DPIA mandatory. | NOYES, AND IT IS DEMONSTRATED | Details of the risk factors identified in the processing that make the DPIA mandatory are included in the DPIA documentation.In particular, it is recommended to make use of the AEPD's [EVALUA-RIESGO RGDP tool for the analysis of risk factors](https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd%22%20%5Ct%20%22https%3A//www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd). |
| 8.3 In accordance with art. 35.1 GDPR, and with the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf), no risk factors have been identified that make the DPIA mandatory, but in the opinion of the data controller the DPIA is necessary and justified on specific grounds. | NOYES, AND IT IS DEMONSTRATED | A DPIA may not be mandatory. Even so, it may be the case that the controller assumes that it is necessary to carry out a DPIA.In that case, the documentation of the DPIA should include details of other risk factors identified in the processing, data protection policies or other elements why the controller considers it necessary to perform the DPIA (e.g. the organisation has a data protection policy that requires the implementation of the DPIA for the processing, there are certification requirements or codes of conduct that require it, transparency or others). |

## Description of the formal risk management process for the rights and freedoms of data subjects (Fifth.5.i and Fifth.5.last paragraph of Instruction 1/2021).

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 9.1 The development of the DPIA documentation takes into account what is indicated by the AEPD in its guides and recommendations, in particular in what is indicated in the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf) (FIFTH.5 last of Instruction 1/2021). | NOYES, AND IT IS DEMONSTRATED | The development of the DPIA documentation must take into account what is indicated by the AEPD in its guides and recommendations, in particular, what is indicated in the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf). |
| 9.2 A reputable methodology has been followed for the risk management process for the rights and freedoms of data subjects. | NOYES, AND IT IS DEMONSTRATED | If the implementation of the DPIA, in addition to the resources of the AEPD, includes additional methodologies for risk management, the scope of these methodologies in the implementation of the DPIA must be indicated in its documentation, as well as the justification for the need to use such methodologies. |
| 9.3 There is an identification of the risk factors for the rights and freedoms of data subjects (art. 35.7.c GDPR). | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation, the identification of inherent and residual risks to the rights and freedoms of data subjects that the processing may entail is carried out. |
| 9.4 An analysis of the possible indirect, collateral or unintended effects of the processing on the rights and freedoms of data subjects has been carried out. | NOYES, AND IT IS DEMONSTRATED | Once compliance with data protection rules has been ensured, in addition to the risk factors inherent to the processing, the possible effects of the processing on the rights and freedoms of individuals should be analysed. |
| 9.5 In the identification of risk factors, their impact has been analysed in relation to possible or potential personal data breach scenarios. | NOYES, AND IT IS DEMONSTRATED | In addition to the risk factors of data processing, account shall also be taken of the negative consequences for the rights and freedoms of natural persons of the loss of confidentiality, integrity and availability of personal data. |
| 9.6 For each risk identified, the impact on the rights and freedoms of data subjects and the likelihood of its occurrence are assessed. | NOYES, AND IT IS DEMONSTRATED | The risk assessment shall be carried out on the basis of quantifiable parameters in terms of impact and likelihood, and the effect of the measures on the risk shall be justified in terms of impact on stakeholders and likelihood of occurrence. |
| 9.7 The measures established on the concept and design of processing to minimise risks to rights and freedoms are identified (art. 25.1 GDPR). | NOYES, AND IT IS DEMONSTRATED | It is recommended to consult section VIII.A of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf). |
| 9.8 Data protection policies and governance measures are identified to minimise risks to rights and freedoms (art. 25.2 GDPR). | NOYES, AND IT IS DEMONSTRATED | It is recommended to consult section VIII.C of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf) and the following resources:* [Default Data Protection Guide](https://www.aepd.es/media/guias/guia-proteccion-datos-por-defecto.pdf)
* [Data protection by default: List of measures](https://www.aepd.es/media/guias/PDpD-listado-medidas.xlsx%22%20%5Ct%20%22https%3A//www.aepd.es/media/guias/PDpD-listado-medidas.xlsx)
 |
| 9.9 Data protection measures are identified by design (art. 25.1 GDPR) to minimise risks to rights and freedoms. | NOYES, AND IT IS DEMONSTRATED | Prior to the development of the product, process or service for which processing may be necessary, data protection measures have been deployed by design, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity of the processing to the rights and freedoms of natural persons.It is recommended to use the AEPD's "[Privacy by Design Guide](https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf)". |
| 9.10 The security measures implemented to minimise the risks to rights and freedoms from personal data breaches are identified (art. 32 and Recital 83 GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation must describe the methodology and ISMS used, as well as its application: inventory of assets, inventory of threats and vulnerabilities associated with each of the identified assets, risk assessment (probability x impact), applicable measures, etc., related to the life cycle of the data in the processing. |
| 9.11 Following the implementation of appropriate measures to avoid and/or mitigate the identified risks, the risk reassessment is carried out taking into account the effect of these measures in relation to the impact and in relation to the likelihood on a stand-alone basis. | NOYES, AND IT IS DEMONSTRATED | A measure or control to mitigate or eliminate a risk will have effects on its impact and/or likelihood of materialisation. These effects shall be justified in order to finally assess the residual risk. |
| 9.12 As a consequence of the implementation of the measures introduced in the processing to avoid and/or mitigate the identified risks, the identification of new risks that could negatively affect the data subjects has been carried out again. | NOYES, AND IT IS DEMONSTRATED | Risk management is an iterative process. The implementation of a risk mitigation measure may in turn lead to the emergence of new risks or unintended consequences for the data subjects. After the implementation of the measures, a new risk identification process must be carried out again. |
| 9.13 An estimate of the level of residual risk achieved by the treatment has been made and each source of risk has been categorised by severity, concluding that the residual risk to the data subjects is low. | NOYES, AND IT IS DEMONSTRATED | In the DPIA documentation the residual risk has to be assessed in accordance with the risk management policy of the organisation, in case the residual risk is low or negligible, the possible prior consultation referred to in Article 36 shall not take place.If there are risks for which the data controller has not been able to take measures, a request for prior consultation as referred to in Article 36 of the GDPR must be made. |
| 9.14 There is an action plan for the implementation of risk management. | NOYES, AND IT IS DEMONSTRATED | Once the manager considers that the residual risk is acceptable, an action plan for the management of the identified risks should be drawn up, which will be associated with the processing life cycle and the data life cycle. |

## Where appropriate, the analysis of the opinion of data subjects or their representatives in relation to the intended processing (Fifth paragraph 5.j of Instruction 1/2021).

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 10.1 Where appropriate, in the process of identifying and assessing the risk to rights and freedoms, the opinion of data subjects or their representatives has been sought and analysed in relation to the intended processing (Art. 35.9 GDPR). | NOYES, AND IT IS DEMONSTRATED | If a consultation process has been carried out with data subjects groups, data subjects or entities representing potential data subjects, the consultation process, the groups and their representativeness, the conclusions and the measures adopted on the basis of these conclusions should be reflected in the DPIA documentation.In doing so, the considerations set out in Chapter XV of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf) have been taken into account. |

## There is an objective and positive assessment of the appropriateness, necessity and proportionality of the treatment (Fifth paragraph 5.k of Instruction 1/2021).

An analysis of necessity and proportionality in relation to the processing operations shall be included.

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 11.1 The adequacy assessment has been carried out in order to evaluate whether the processing, as it stands, is effective enough to achieve its intended purpose. | NOYES, AND IT IS DEMONSTRATED | Thresholds of treatment effectiveness shall be determined in the DPIA documentation by establishing objective, qualitative, evidence-based thresholds of treatment effectiveness.These effectiveness thresholds shall be reviewed in an equally objective manner throughout the life cycle of the treatment. The treatment, throughout its life cycle, shall be suitable to the extent that it meets the established thresholds. |
| 11.2 The necessity, proportionality and adequacy analysis is carried out in relation to the personal data used and the processing operations. | NOYES, AND IT IS DEMONSTRATED | The necessity, proportionality and adequacy analysis described in the DPIA documentation has been taken into account for each of the processing operations and in relation to the personal data used in each of the identified processing operations.Chapter XIII of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf) has been taken into account for this analysis. |
| 11.3 There is an objective evaluation that demonstrates that the processing passes the adequacy assessment according to the criteria in section XIII.B of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation should detail the evaluation process, and not only its conclusion, which has determined that the processing is fit for purpose. It should detail whether the processing addresses specific objective gaps, demands, requirements, obligations or opportunities and can achieve the proposed objectives with sufficient effectiveness. |
| 11.4 There is an objective assessment that demonstrates that the processing passes the necessity assessment according to the criteria in section XIII.C of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation should detail the evaluation process, and not only its conclusion, which has determined that the intended purpose cannot be achieved in a less harmful or invasive way, i.e. there is no alternative processing that is equally effective in achieving the intended purpose. |
| 11.5 There is an objective evaluation that demonstrates that the processing passes the proportionality assessment in the strict sense according to the criteria in section XIII.D of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf). | NOYES, AND IT IS DEMONSTRATED | The DPIA documentation should detail the evaluation process, and not only its conclusion, which has determined that the seriousness of the risk to the rights and freedoms of the processing, and its intrusion on privacy, is appropriate to the intended purpose and proportionate to its urgency and severity. It should detail the balancing of the benefit that the processing, from a data protection point of view, provides to society while maintaining a balance with the impact on other fundamental rights (Recital 4 GDPR). |

## Criteria for reassessing the DPIA and, where appropriate, for the expiry of processing. (Quinto.5.l of Instruction 1/2021)

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 12.1 The action plan for the management of risks to rights and freedoms reflects the actions for the review and updating of the measures determined in the DPIA. (Art. 24 GDPR) | NOYES, AND IT IS DEMONSTRATED | Taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the controller shall implement technical and organisational measures and such measures shall be reviewed and updated as necessary. |
| 12.2 The action plan, data protection policies and/or risk management for rights and freedoms reflect the regular reassessment of the necessity of the processing and the restriction of the data used (Art. 24 and 5.e, Recital 78 GDPR). | NOYES, AND IT IS DEMONSTRATED | For each data or set of data, policies may be established to ensure the necessity of the processing throughout its life cycle, as well as the technical and organisational mechanisms that may be necessary to limit the use of data previously required for processing. |
| 12.3 Expiry clauses are included in the data protection policies, the action plan and/or in the definition of the processing (section XIII.C.1 of the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)). | NOYES, AND IT IS DEMONSTRATED | Processing may be needed on a short-term basis to address a particular problem. Once the situation has been resolved, the processing may no longer be necessary, which in practice means that limitations to continued processing are included in the analysis of need. |

## Additional Documentation (Fifth.5.m of Instruction 1/2021)

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 13.1 The Supervisory Authority is given access to all documentation to ensure that the information provided is complete and accurate (art. 36.3 GDPR). | NOYES, AND IT IS DEMONSTRATED | If necessary, the information that the data controller deems necessary must be made available to the Supervisory Authority, without prejudice to the powers that Article 58 of the GDPR grants to the Supervisory Authority itself.Incomplete or inaccurate information, in addition to possible regulatory non-compliance, may be grounds for rejection of the prior consultation by the Supervisory Authority. |

## Compliance with the requirements for submission of prior consultation (Fifth.6, 7 of Instruction 1/2021)

|  |  |  |
| --- | --- | --- |
| **ELEMENTS OF VERIFICATION** | **CHECK** | **COMMENTS**(replace these comments with the appropriate ones in each case) |
| 14.1 The prior consultation is signed by the controller. | NOYES, AND IT IS DEMONSTRATED | Prior consultation is different from the DPIA, even if it is carried out as a consequence of the latter.It is the controller, through its representatives, who must carry it out. |
| 14.2 The prior consultation is sent via the prior consultation channel provided by the AEPD at its website. | NOYES, AND IT IS DEMONSTRATED | The entry of a prior consultation must be made through the specific channel set up by the AEPD.Requests for prior consultation through channels other than the one specifically established in the AEPD's website will lead to the rejection of the request. |
| 14.3 The request for prior consultation includes the DPIA (Art. 36.3 GDPR). | NOYES, AND IT IS DEMONSTRATED | The DPIA will have to comply formally with the formal requirements of this checklist and substantively with the requirements developed in the [Guide](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf). |
| 14.4 This checklist is completed with evidence to support the answers. | NOYES, AND IT IS DEMONSTRATED | Strict compliance with this checklist will allow you to ensure that the prior consultation request formally meets the requirements to be considered as such. |

# Guides and tools

The AEPD has made available to data controllers and data processors a set of guides and tools to assist in risk management for the rights and freedoms of data subjects, as well as for the process of implementing the DPIA. This material is available on the AEPD website [www.aepd.es](http://www.aepd.es/) and, in particular, in the following sections of the website:

* [Fulfil your duties](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes)
* [Innovation and technology](https://www.aepd.es/en/areas/innovation-and-technology)
* [Guides](https://www.aepd.es/en/guias-y-herramientas/guias)
* [Tools](https://www.aepd.es/en/guides-and-tools/tools)

[In particular, the DPIA and the relevant prior consultation must take into account the following provisions of the AEPD:](https://www.aepd.es/en/guides-and-tools/tools)

* [Risk management and impact assessment in the processing of personal data](https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf)
* [List of tables from the Risk Management and Impact Assessment guide in editable format](https://www.aepd.es/es/documento/relacion-tablas-guia-riesgo-eipd-tablas.odt)
* [Lists of types of data processing requiring a DPIA (Art. 35.4)](https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf)
* [Indicative list of types of data processing which do not require a data protection impact assessment (Art. 35.5)](https://www.aepd.es/sites/default/files/2019-09/ListasDPIA-35.5l.pdf)
* [AEPD Instruction 1/2021 on guidelines regarding the Agency's advisory function. Chapter IV: Prior Consultation](https://www.boe.es/boe/dias/2021/11/05/pdfs/BOE-A-2021-18134.pdf)
* [Data Protection Impact Assessment (DPA) report template for Public Administrations](https://www.aepd.es/sites/default/files/2020-03/modelo-informe-EIPD-AAPP.rtf)
* [Data Protection Impact Assessment (DPA) report template for the Private Sector](https://www.aepd.es/sites/default/files/2020-03/modelo-informe-EIPD-sector-privado.rtf)
* [EDPS: Guidelines on assessing the proportionality of processing in policies and legislative measures](https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf)
* [EDPS: Guidelines on assessing the necessity for processing in policies and legislative measures](https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf)
* [EVALUA-RIESGO Tool for risk factor analysis](https://www.aepd.es/en/guias-y-herramientas/herramientas/evalua-riesgo-rgpd)
* [A tool to help companies that carry out low-risk processing of personal data to comply with the GDPR: FACILITA RGPD](https://www.aepd.es/en/guides-and-tools/tools/facilita-rgpd)
* [A tool to help entrepreneurs and technology start-ups to comply with data protection regulations: FACILITA EMPRENDE](https://www.aepd.es/en/guias-y-herramientas/tools/facilita-emprende)
1. Article 24.1 GDPR: *"Taking into account the nature, scope, context and purposes of the processing, as well as risks of varying likelihood and likelihood and severity to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures in order to ensure and be able to demonstrate that the processing is in compliance with this Regulation. Such measures shall be reviewed and updated whenever necessary."* [↑](#footnote-ref-1)