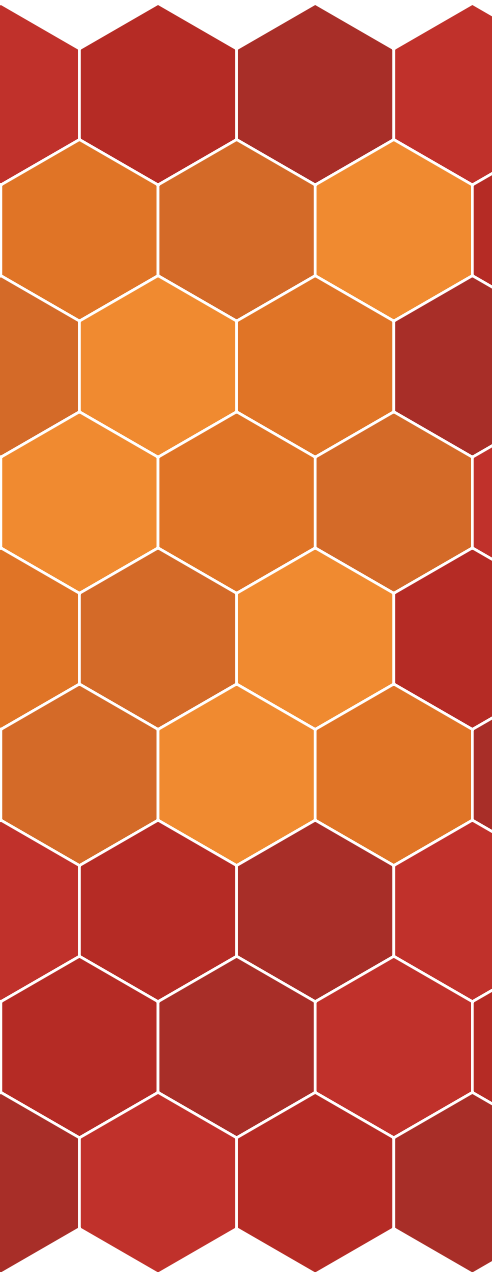


# Guidelines for an Integrated Plan for the DPIA-FRIA

**October 2026**

DPD
en xarxa

# Contents

Presentation ..... 4

1. The main blocks of the DPIA and their integration with the FRIA ..... 5

    1.1 The systematic description ..... 5

    1.2 The assessment ..... 6

    1.3 Mitigation measures ..... 9

2. The integrated DPIA-FRIA workflow and model design ..... 10

Coordinators:

Alessandro Mantelero and Joana Marí

Participants:

Aida Mariscal (Telecommunications and Information Technologies Centre)
Albert Portugal (Consortium of University Services of Catalonia)
Albert Serra (Catalan Data Protection Authority)
Alessandro Mantelero (Polytechnic University of Turin)
Carles Garcia (Catalan Data Protection Authority)
Carlos López (Catalan Data Protection Authority)
Cristina Guzmán (Universitat Politècnica de Catalunya – BarcelonaTech (UPC))
Esther Garcia (CaixaBank, SA)
Irma Choy (AOC Consortium)
Joana Judas (Catalan Data Protection Authority)
Joana Marí (Catalan Data Protection Authority)
M. Ascensión Moro (Sant Feliu de Llobregat City Council)
M. Ester Santiago (Barcelona City Council)
Maria José Campo (TIC Salut i Social Foundation)
Maria José Candial (Barcelona City Council)
Mariona Perramon (Consortium of University Services of Catalonia)
Mireia Bosch (Department of Justice and Democratic Quality)
Patricia Lozano (Universitat Oberta de Catalunya)
Rosa Parrilla (Department of the Presidency)
Roser Bellido (Department of Social Rights and Inclusion)
Ruben Ortiz (University of Barcelona)
Sara Hernández (TIC Salut i Social Foundation)

**CC BY-NC-ND** | Barcelona, 2026

The content of this document is the property of the Catalan Data Protection Authority and is subject to the Creative Commons BY-NC-ND licence, https://creativecommons.org/licenses/by-nc-nd/4.0/.

Authorship of the work must be acknowledged by including the following notice:
Work owned by the Catalan Data Protection Authority.
Licensed under the CC BY-NC-ND licence.

Notice: when the work is reused or distributed, the terms of the licence must be clearly indicated.

Legal notice: The opinions expressed in this document are the responsibility of their authors and do not necessarily reflect the official opinion of the APDCAT. The Catalan Data Protection Authority, the authors and the members of the working group accept no responsibility for the possible consequences of the actions of natural or legal persons arising from any information contained in this document.

*This is an unofficial English translation of the original Catalan document. In case of doubt, the original prevails.*

# Presentation

In 2026 we celebrated the tenth anniversary of the General Data Protection Regulation. There is little left to say that has not been said before, but it is clear that it was a decisive piece of legislation in consolidating the fundamental right to data protection, both at European and international level.

Indeed, it is the foundation on which the entire European data strategy has been built. Thus, the Artificial Intelligence Act, of 2024 and amended in 2026, mentions it on several occasions throughout its articles: on the one hand, stating that it does not displace it (recital 10 and Article 2.7); on the other, strengthening the role of data protection supervisory authorities, in articles such as 5, 57, 74 or, once fundamental rights protection authorities have been designated, 77. And, finally, Article 27 deserves special mention.

This article regulates fundamental rights impact assessments for artificial intelligence systems (FRIA) and establishes the relationship between this assessment and the data protection impact assessment under the GDPR and Directive (EU) 2016/680 (DPIA). In the 2026 wording, following the omnibus reform approved by the European Union, it provides that between the two assessments either cross-references or the relevant parts of the DPIA may be included in the FRIA. Both regulations are therefore complementary.

But there is a step from the rule to practice. For that reason, the Catalan Data Protection Authority set out to fill two gaps: the first, how to carry out a fundamental rights impact assessment; the second, how to effectively integrate the two assessments.

We answered the first gap in January 2025, with the presentation of the Catalan FRIA model: a pioneering methodology tested with several use cases. It was the result of the work of a working group led by Professor Alessandro Mantelero, of the Polytechnic University of Turin, within the framework of DPD en Xarxa, the learning community promoted by the APDCAT. This model was one of the first adopted by the European Union Agency for Fundamental Rights. On 7 October 2026, the FRIA tool was presented as an implementation of this FRIA model, allowing the impact assessment to be carried out in an automated and agile way.

We fill the second gap with these guidelines, which are the result of the work of the same working group, which did not stop and has continued working to provide DPOs and organisations with a new resource that will facilitate regulatory compliance.

At the APDCAT, we remain committed to guaranteeing the right to data protection and the rest of fundamental rights. And we will continue working on it, hand in hand with the great professionals we have in Catalonia.

**Meritxell Borràs i Solé**
Director
Catalan Data Protection Authority

# 1. The main blocks of the DPIA and their integration with the FRIA

The following sections examine the main elements of the DPIA as established in Article 35 of the GDPR. They describe the content of the DPIA on the basis of international practice and the experience of the public sector in Catalonia. Using the APDCAT DPIA template, guidelines are provided to identify the key elements to be included in each phase, with the aim of creating a DPIA that can easily complement the FRIA required by the AI Act.

The resulting model is not intended to replace the APDCAT DPIA template or the existing templates developed by various institutions, but to present an agile model that can be easily integrated with the FRIA template adopted by the APDCAT (on 7 October 2026 the FRIA tool was presented as an implementation of this FRIA model, allowing the impact assessment to be carried out more efficiently).

The new template allows users to extend the DPIA section in order to include a broader assessment of compliance with the provisions of the GDPR in general and, in particular, when AI is incorporated into personal data processing.

This simplification exercise has been necessary in view of Article 27.4 of the AI Act, which states:

> *"4. If any of the obligations laid down in this Article are already met through the data protection impact assessment carried out under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the deployer may, when carrying out the fundamental rights impact assessment referred to in paragraph 1 of this Article, include cross-references to the relevant sections of that data protection impact assessment or include the relevant parts of it in the fundamental rights impact assessment."*

The methodology is structured around two parts common to both assessments which, in an integrated model, can be examined only once, with results that can be used for both the DPIA and the FRIA. This analysis is crucial to avoid assessing the same elements twice (for example, the context of use) and to create a coherent flow of information between the two assessments.

## 1.1 The systematic description

This is the first part of both the DPIA and the FRIA. It consists of analysing the needs and describing the planned solutions that will be developed, with reference to their context of use. Users of the impact assessment tool must be given preliminary general information on the nature and purpose of the assessment and on the general concepts of risk-based assessment, which are present in both the GDPR and the AI Act.

As regards the description of the planned solutions, projects involving the use of personal data, as well as those involving AI, must describe how both the data and the AI are used. To this end, detailed information must be provided on the nature of the data and its processing, which will be integrated with the information on the AI system used. Likewise, information is needed on the persons directly involved in the development of the project and their role under the GDPR (controller, joint controller, processor, sub-processor) and the AI Act (provider, deployers), the

possible categories of affected rights-holders, and the contexts of use.

## 1.2 The assessment

As regards the assessment phase, it should be noted that the DPIA and the FRIA are legal obligations with a limited scope, defined, respectively, by Article 35 of the GDPR and Article 27 of the AI Act. However, in the field of data protection, as in that of AI, prior risk assessment has a scope that goes beyond the regulated impact assessments.

Under the GDPR, risks must be taken into account when applying the Regulation, even if they do not entail a high risk to the rights and freedoms of natural persons. In these cases too, it remains necessary to properly apply all the principles set out in Article 5 of the GDPR and the relevant provisions of the Regulation, in order to minimise any impact, even the least significant, on the right to data protection and other fundamental rights. A general risk assessment is therefore inherent in all processing activities, whereas a formal DPIA is mandatory only in high-risk cases.[1]

The same applies to the FRIA. Although it is limited to certain categories of deployers and certain situations, the guaranteed protection of fundamental rights requires a duty to actively protect these rights, and a FRIA is a useful tool to achieve this objective. Moreover, the FRIA, as a methodology for assessing the impact on fundamental rights, can also be used by AI providers to comply with Article 9 as regards the risks they pose to fundamental rights and, in general, by any entity that incorporates AI systems into its organisation, given that in the context of the European Union the guarantee and protection of the fundamental rights set out in the Charter of Fundamental Rights of the European Union is common to any action.

As regards strict compliance with the GDPR and the AI Act, a model integrating the DPIA and the FRIA requires a prior analysis of the legal requirements established by these two regulations, in order to determine the cases in which both are mandatory. This assessment is carried out in section 2 of the assessment model (Need to carry out a DPIA and a FRIA).

As regards the assessment of the risk to the “rights and freedoms of natural persons” (Article 35 of the GDPR) and the “impact on fundamental rights” (Article 27 of the AI Act), there are differences because the European AI Regulation, in Article 1, refers to the “protection of [...] the fundamental rights enshrined in the Charter”. However, beyond the legal qualification of these rights, the methodological approach is the same: it focuses on risk in terms of harm to these rights, taking into account the likelihood of harm occurring and its severity.[2]

As can be seen in the following tables, taken from the CNIL data protection impact assessment template[3] and the APDCAT FRIA[4], the risk assessment methodology is aligned in the same way in both instruments.

[1] See also Article 29 Data Protection Working Party (note 2), 8 (“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.”).

[2] See Article 3(2) of the AI Act; Article 25(1) and recital 75 of the GDPR. According to recital 76 of the GDPR, “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.”

**Table 3. CNIL PIA**

PIA, templates — February 2018 edition

## 3.2 Risk assessment: potential privacy breaches

Analysis and assessment of risks

| Risk | Main risk sources | Main threats | Main potential impacts | Main controls reducing the severity and likelihood | Severity | Likelihood |
|---|---|---|---|---|---|---|
| Illegitimate access to data | | | | | | |
| Unwanted change of data | | | | | | |
| Disappearance of data | | | | | | |

Assessment of the risks

| Risks | Acceptable/can be improved on? | Corrective controls | Residual severity | Residual likelihood |
|---|---|---|---|---|
| Illegitimate access to data | *[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]* | *[Where applicable, he shall indicate here any additional controls that would prove necessary.]* | | |
| Unwanted change of data | *[The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.]* | *[Where applicable, he shall indicate here any additional controls that would prove necessary.]* | | |

[3] See CNIL (note 7), 20.

[4] See Catalan Data Protection Authority (note 6), 19.

**Table 4. APDCAT FRIA**

## Table 2A. Risk management (I)

| Rights/freedoms affected | Likelihood | Severity | Overall impact | Measures to prevent/mitigate impacts |
|---|---|---|---|---|
| | | | | |
| | | | | |

## Table 3A. Risk management (II)

| Rights/freedoms affected | Likelihood (residual) | Severity (residual) | Residual impact |
|---|---|---|---|
| | | | |
| | | | |

In accordance with the general risk assessment methodology, **the likelihood and severity of possible harms are examined** on the basis of the project design, possible mitigation measures are envisaged, and a new assessment is carried out to define the impact of these measures and the residual risks. This iterative process is consistent with the risk-based approach adopted by both the DPIA and the FRIA.

However, whereas the DPIA analyses the various risks to a single right, reflecting the procedural nature of data protection in terms of possible violations (for example, unauthorised access to data or unwanted changes), the FRIA considers each affected right in its entirety, without identifying subsets of risks for each type of potential harm. This is also because the protection of fundamental rights other than the right to data protection does not have a similar procedural nature and, in their respective regulations, is based on the definition of a specific scope of protection and on the prohibition of interfering with it, except where other legal goods and interests prevail in accordance with the law.

Therefore, in order to align the DPIA and the FRIA, there is no need to revise the matrices used in the DPIA to assess the level of risk to data protection, since these matrices continue to form part of the general assessment of the impact on this right.

Nevertheless, the mitigation measures adopted in the area of data protection may also benefit other rights, which must be taken into account in terms of the controls established, by updating section C of the FRIA questionnaire.

In addition, it must be borne in mind that the processing of personal data may generate risks to other rights and freedoms of individuals, beyond the right to personal data protection itself. The DPIA can therefore also help to identify potential impacts on other rights arising from the processing carried out and, in particular, from the use made of AI.

## 1.3 Mitigation measures

The final block of the DPIA consists of identifying the most appropriate mitigation measures to reduce the impact on data protection.

In accordance with Article 35(7)(d), these measures are those “envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.”

These mitigation measures may include the elements of GDPR compliance that can contribute to reducing risk. Moreover, these elements are also relevant from the FRIA perspective, as they can help reduce negative effects on other rights and freedoms.

Data quality, for example, can reduce bias and negative effects on the right to non-discrimination, while human oversight[5] can be effective in data-based decision-making, not only in terms of GDPR compliance but also as an intervention that mitigates the impact on other affected rights.[6]

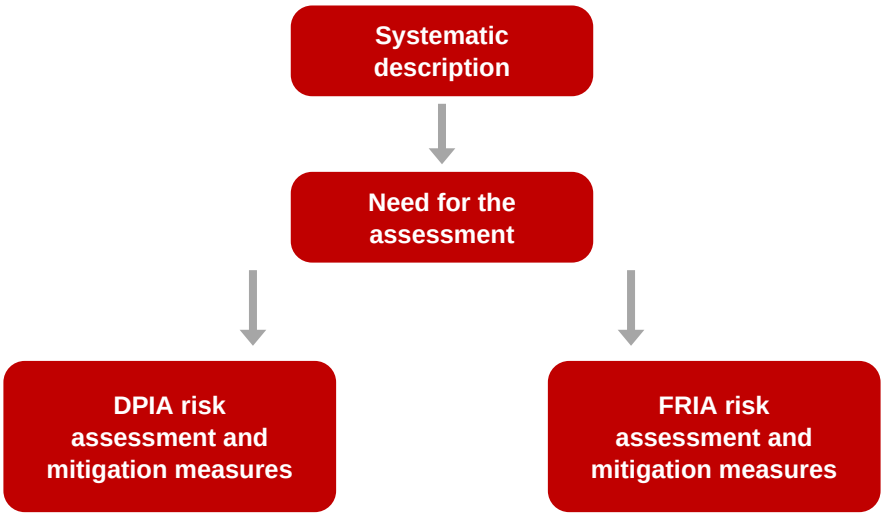
In relation to the above, the various questions on these different aspects included in the DPIA must be reframed within the logic of the possible measures to be adopted to mitigate risks, rather than as elements of a compliance check.

[5] See also Article 14 of the AI Act.

[6] The same consideration can be applied to transparency, which is a factor that makes it possible to understand the possible negative consequences of the use of data, also in the context of AI, and which can be combined with the transparency obligations laid down in the AI Act (see also Article 13 of the AI Act). Proper compliance with the transparency obligations of AI system providers established in the AI Act is essential for compliance with the controller’s obligations under the GDPR.

## 2. The integrated DPIA-FRIA workflow and model design

In accordance with the considerations set out in the preceding sections, the general workflow of the DPIA-FRIA model template can be described as shown in the following diagram:




### Access to the DPIA-FRIA Template