Guidelines for an integrated DPIA-FRIA plan

October 2026

DPD en xarxa

Index

Introduction 4

1. The main sections of the DPIA and its integration with the FRIA 5
    1.1 The systematic description 5
    1.2 The assessment 6
    1.3 Mitigation measures 8

2. The integrated DPIA-FRIA workflow and model design 9

Coordinators:

Alessandro Mantelero and Joana Marí

Participants:

Aida Mariscal (Centre for Telecommunications and Information Technologies)

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 (Polytechnic University of Catalonia – 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 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 (Open University of Catalonia)

Rosa Parrilla (Department of the Presidency)

Roser Bellido (Department of Social Rights and Inclusion)

Ruben Ortiz (University of Barcelona)

Sara Hernández (TIC Salut Social Foundation)



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/.

The authorship of the work must be acknowledged by including the following mention:
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 any consequences arising from actions taken by individuals or legal entities on the basis of information contained in this document.

Introduction

In 2026, we celebrated the tenth anniversary of the General Data Protection Regulation. There is little to add to what has already been said, but it is clear that the Regulation played a decisive role in consolidating the fundamental right to data protection, both in Europe and internationally.

In fact, it is the foundation upon which the entire European data strategy has been built. Thus, the Artificial Intelligence Act, adopted in 2024 and amended in 2026, refers to it on several occasions: first, by stating that it does not supersede it (recital 10 and Article 2(7)); and second, by strengthening the role of data protection supervisory authorities in provisions such as Articles 5, 57, 74 and 77, the latter concerning designated authorities responsible for protecting fundamental rights. Finally, Article 27 is particularly noteworthy.

This article regulates fundamental rights impact assessments for artificial intelligence systems (FRIAs) and establishes the relationship between these assessments and data protection impact assessments (DPIAs) under the GDPR and Directive (EU) 2016/680. And in the 2026 version, following the omnibus reform approved by the European Union, it provides that cross-references or relevant parts of the DPIA may be included in the FRIA. Therefore, both regulations are complementary.

But putting the rules into practice is another matter. And, for this reason, from the Catalan Data Protection Authority we 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 addressed the first gap in January 2025 with the presentation of the Catalan FRIA model: a pioneering methodology tested in various use cases. It was the result of the work of a working group led by Professor Alessandro Mantelero, from 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 to be adopted by the European Union Agency for Fundamental Rights. On 7 October 2026, the FRIA tool was presented, based on this FRIA model, enabling impact assessments to be carried out automatically and efficiently.

These guidelines address the second gap. They are the result of the work of the same working group, which has continued its efforts to provide DPOs and organisations with a new resource to facilitate regulatory compliance.

At the APDCAT, we remain committed to safeguarding the right to data protection and other fundamental rights. And we will continue working towards this goal, alongside the excellent professionals we have in Catalonia.

Meritxell Borràs i Solé
Director
Catalan Data Protection Authority

1. The main sections of the DPIA and its integration with the FRIA

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

The resulting model does not intend to replace the APDCAT DPIA template or existing templates developed by various institutions, but rather 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 for this FRIA model, which allows impact assessments to be carried out more efficiently).

The new template allows users to expand the DPIA section 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 what is established in Article 27.4 of the AI Act, where it is indicated that:

> "4. If any of the obligations laid down in this Article are already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the deployer may, when conducting 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 thereof in the fundamental rights impact assessment."

The methodology is structured around **two parts that are common to both assessments**. In an integrated model, these need only be examined once, with the results then being used for both the DPIA and the FRIA. This analysis is crucial in order to avoid duplicating the assessment of the same elements twice (for example, with regard to the analysis of the context of use) and to ensure 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 carrying out an analysis of 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 provided with preliminary information on the nature and purpose of the assessment and the general concepts of risk-based assessment, which are found in both the GDPR and the AI Act.

Regarding 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. For this reason, detailed information must be provided on the nature of the data and how it is processed, together with information on the AI system used. Similarly, 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, deployer), the possible

categories of rights holders affected and the contexts of use.

1.2 The assessment

Regarding 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 the field of AI, prior risk assessment goes beyond the scope of the impact assessments required by law.

Under the GDPR, risks must be taken into account when applying the Regulation, even if they do not pose a high risk to the rights and freedoms of natural persons. Even in these cases, it remains necessary to properly apply all the principles established in Article 5 of the GDPR and the relevant provisions of the Regulation, with the aim of minimising any impact, however minor, on the right to data protection and other fundamental rights. Therefore, a general risk assessment is inherent to all processing activities, whereas a formal DPIA is only mandatory in cases of high risk.[1]

The same applies to the FRIA. Although it is limited to certain categories of deployers and certain situations, ensuring the protection of fundamental rights requires active measures to safeguard these rights, and an FRIA is a useful tool for achieving this objective. Furthermore, the FRIA methodology for assessing the impact on fundamental rights **can also be used by AI providers** to comply with Article 9 regarding the risks posed to fundamental rights and, more generally, by any organisation that incorporates AI systems, since the obligation to guarantee and protect fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union, applies to all activities within the EU.

Regarding strict compliance with the GDPR and the AI Regulation, a model that integrates the DPIA and the FRIA requires a prior analysis of the legal requirements established by these two regulations, in order to determine the scenarios in which both are mandatory. This assessment is carried out in section 2 of the assessment model (Need to carry out a DPIA and an FRIA).

Regarding the risk assessment for 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 classification of these rights, the methodological approach is the same: it focuses on risk in terms of harm to these rights, taking into account the probability of harm occurring and the severity of that harm.[2]

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

---

[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 data processing."
[3] See CNIL (note 7), 20.
[4] See Catalan Data Protection Authority (note 6), 19.

Table 3. CNIL PIA

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.*]		

Table 4. APDCAT FRIA

Taula 2A. Gestió de riscos (I)

Drets/llibertats afectats	Probabilitat	Gravetat	Impacte global	Mesures per prevenir/mitigar els impactes

Taula 3A. Gestió de riscos (II)

Drets/llibertats afectats	Probabilitat (residual)	Gravetat (residual)	Impacte residual

In accordance with the general risk assessment methodology**, the probability and severity of potential harm are examined** based on the project design, potential 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, while the DPIA analyses the various risks to a single right, reflecting the procedural nature of data protection in terms of potential breaches (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 the same procedural nature and, under the respective legal frameworks, is based on defining a specific scope of protection and prohibiting interference with those rights, unless where other legally protected rights and interests take precedence under the law.

Therefore, to align the DPIA and the FRIA, it is not necessary to revise the matrices used in the DPIA to assess the level of risk to data protection, as these matrices continue to form part of the general impact assessment on this right.

However, mitigation measures adopted in the field of data protection may also benefit other rights. This should be taken into account when considering the controls established, by updating section C of the FRIA questionnaire.

It should also be borne in mind that the processing of personal data can pose risks to other rights and freedoms of individuals, beyond the right to the protection of personal data itself. Therefore, the DPIA can also help identify potential impacts on other rights arising from the processing carried out and, in particular, from the use of AI.

1.3 Mitigation measures

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

In accordance with Article 35, paragraph 7, letter *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 elements of GDPR compliance that can contribute to reducing risk. Furthermore, these elements are also relevant from the perspective of the FRIA, as they can help to 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-driven decision-making, not only

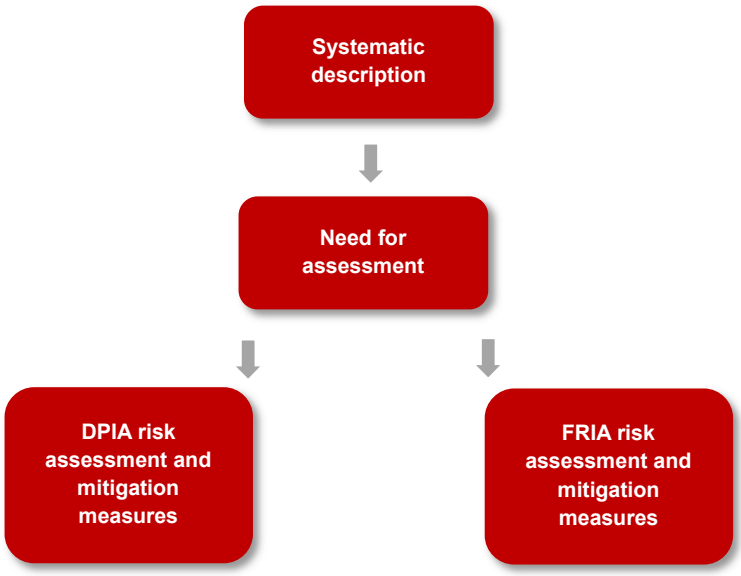
[5] See also Article 14 of the AI Act.

in terms of GDPR compliance, but also as an intervention that mitigates the impact on other affected rights.[6]

In light of the above, the various questions concerning these aspects included in the DPIA must be reconsidered in terms of the possible measures to be adopted to mitigate risks, rather than as elements of a compliance check.

2. The integrated DPIA-FRIA workflow and model design

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



DPIA-FRIA Template

[6] The same consideration applies to transparency, which helps us understand the potential negative consequences of data use, including in the context of AI, and can be combined with the transparency obligations laid down in the AI Act; see also Article 13 of the AI Act. Compliance with the transparency obligations of AI system providers, as set out in the AI Act, is essential for controllers to fulfil their GDPR obligations.


DPD
en xarxa