Nemko Digital



Two Assessments, One Framework:

Integrating DPIA and FRIA Under the EU AI Act

For nearly a decade, the Data Protection Impact Assessment (DPIA) has been the default lens through which organisations think about "risk assessment" in digital projects. Under Article 35 of the General Data Protection Regulation ("GDPR"), a DPIA is required whenever processing is "likely to result in a high risk to the rights and freedoms of natural persons" and AI-driven profiling, large-scale monitoring, and automated decision-making sit squarely within that category.

The EU Artificial Intelligence Act (Regulation (EU) 2024/1689, "AI Act") introduces a second, related but distinct obligation: the Fundamental Rights Impact Assessment ("FRIA"), set out in Article 27. From 2 August 2026, certain deployers of high-risk AI systems will need to complete a FRIA before first use.

Many organisations may view the FRIA as simply a "DPIA for AI." That approach is misleading. A more accurate view is that both assessments stem from the protection of fundamental rights under the Charter of Fundamental Rights of the European Union. The key compliance question is therefore not whether to conduct a DPIA or a FRIA, but how to create a unified assessment framework that satisfies both without duplication.

This article explains the legal basis for that approach, where DPIAs and FRIAs overlap, where they differ, and how a unified methodology can work in practice.

The DPIA: a data centric risk lens

Article 35 GDPR requires a DPIA where processing using new technologies is likely to result in high risk to individuals' rights and freedoms, with profiling, automated decision-making, and large-scale processing of special category data named as triggering criteria. The European Data Protection Board's (EDPB) set out nine criteria for assessing "likely high risk," including evaluation or scoring, automated decision-making with legal or similarly significant effect, and the use of innovative technology.

The DPIA is centered in the concept of "personal data." It examines what data is being processed, on what legal basis, with what safeguards, and what residual risk remains to data subjects' rights under the GDPR rights such as access, rectification, erasure, and the right not to be subject to solely automated decisions under Article 22. It is a rigorous, well-understood instrument. But it was drafted in 2016, before large-scale machine learning systems were a mainstream deployment reality, and its statutory vocabulary reflects that: "personal data," "data subject," "processing."

The FRIA: a rights-centric risk lens

Article 27 of EU AI Act takes a structurally different starting point. Certain deployers of high-risk AI systems must assess the impact of those systems on fundamental rights before deployment.

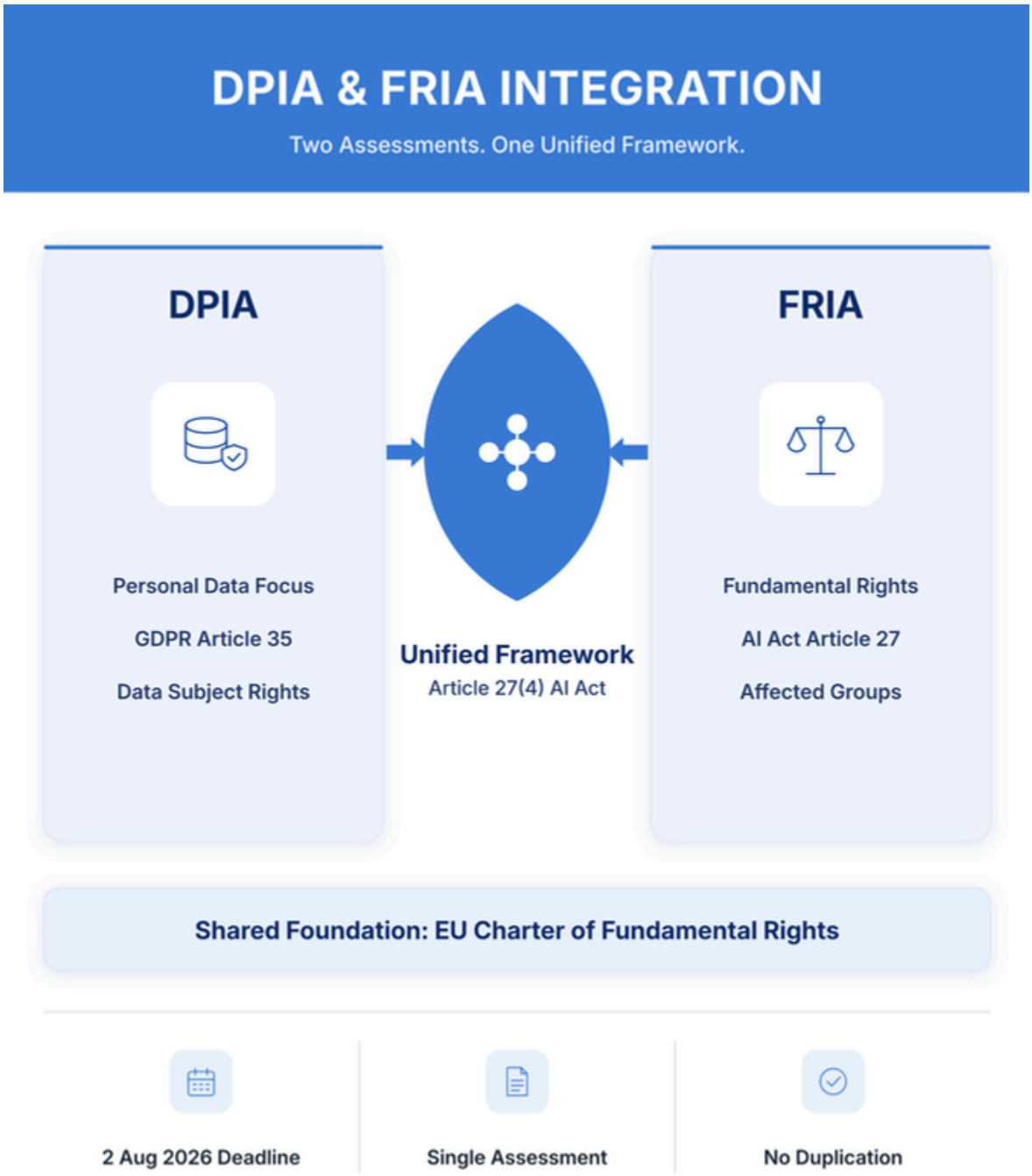
The assessment must cover the intended purpose of the system, its use, affected persons or groups, potential harms, human oversight measures, and actions to be taken if risks materialise. Deployers must also notify the relevant market surveillance authority. Two features distinguish the FRIA from the DPIA in ways that matter for compliance design:

First, scope. The FRIA is not limited to personal data processing. It addresses a wider range of Charter rights, including non-discrimination, human dignity, freedom of expression, and access to justice. An AI recruitment system may therefore raise fundamental rights concerns even where its data processing complies with GDPR requirements.

Second, population. While a DPIA focuses on data subjects, a FRIA considers groups likely to be affected by an AI system. This can include individuals impacted by the system's outcomes even if their personal data was never processed.



Where the legislator has already built the bridge



DPIA and FRIA are different but aligned under Article 27(4) of the EU AI Act. Both protect fundamental rights under the EU Charter—here's how a unified framework works in practice.

The AI Act itself draws the connection. Article 27(4) provides that where FRIA obligations are already met through a DPIA conducted under Article 35 GDPR, the FRIA "shall complement that data protection impact assessment." The legislative intent is that the two assessments should be conducted as a single integrated exercise where they overlap, rather than duplicated as parallel exercises.

Recital 96 adds that deployers conducting a FRIA "could involve relevant stakeholders, including representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations." This is not a binding requirement but a best practice favoured by the legislator, particularly for public-sector deployers. The AI Office is expected to publish a standard FRIA template. Until then, organisations should treat unofficial templates as provisional rather than authoritative tools.

Building an Effective Monitoring Capability

In practice, integrating DPIA and FRIA requirements can be achieved through four components:

01.

A shared intake and screening stage: Before drafting either document, identify (a) whether personal data is processed (triggering Article 35 GDPR analysis) and (b) whether the system is "high-risk AI systems" under Article 6 and Annex III of the AI Act, and if so, whether the deployer falls within the categories captured by Article 27(1). Many organisations will find both triggers apply to the same system simultaneously.

02.

A single descriptive section: Document the system's purpose, timeframe, affected persons rather than repeating information across assessments.

03.

Two distinct risk-analysis tracks within one document: Maintain a GDPR-rights track (lawfulness, fairness, transparency, data subject rights, Article 22 safeguards) and a Charter-rights track (non-discrimination, human dignity, access to effective remedy, freedom of expression, as relevant to the use case). Map both tracks against the same affected-population analysis so risks are not assessed in isolation from one another.

04.

A unified mitigation and governance section: Cover oversight measures, complaint mechanisms, escalation procedures, and risk controls that satisfy both GDPR and AI Act requirements.

This approach is more than an administrative convenience. Separate assessments can create gaps: privacy teams may focus on data protection issues while overlooking group-level discrimination, whereas AI teams may identify bias risks without connecting them to legal rights. A unified approach helps bridge those perspectives before deployment.

The DPIA: a data centric risk lens

The DPIA and FRIA cannot always be merged completely. Article 27 applies to a narrower category of deployers than Article 35 GDPR. Many organisations may be required to conduct a DPIA without being subject to a FRIA.

Assuming that one assessment automatically satisfies the other can therefore create compliance risks. Organisations should first determine which obligations apply before adopting any methodology.

Conclusion

The relationship between DPIA and FRIA is neither substitution nor duplication. Both derive from the protection of fundamental rights but operate through different legal instruments: GDPR for personal data processing and the Regulation (EU) 2024/1689 for broader AI-related risks.

Organisations that treat them as entirely separate exercises may duplicate effort while producing fragmented results. Those that adopt a unified rights-based framework, consistent with Article 27(4) AI Act, are likely to achieve more coherent compliance and demonstrate that fundamental rights have been meaningfully assessed rather than merely documented.

About the author



Srushti Gosavi

Srushti Gosavi is a privacy and AI governance professional with experience in legal research, compliance, and regulatory technology. Through her work in AI and privacy compliance, as well as her research on the GDPR, EU AI Act, and emerging digital regulations, she focuses on translating complex legal requirements into practical governance frameworks. Her work supports the responsible adoption of AI and data-driven technologies while helping organizations navigate evolving regulatory landscapes.

Nemko Digital