

## Feedback on the EDPB DPIA Template – Public Consultation

I welcome the initiative of the European Data Protection Board to issue a Data Protection Impact Assessment (DPIA) template. The effort contributes to aligning expectations among controllers and fostering greater coherence in the application of Article 35 GDPR, particularly in cross-border processing contexts where fragmentation between supervisory authorities remains observable.

From a practitioner's perspective, the introduction of a common reference point is valuable. Over time, DPIA practices have varied significantly across organisations and jurisdictions, both in structure and depth. The template's overall architecture reflects a familiar and operationally sound logic, broadly aligned with approaches previously promoted by supervisory authorities such as the CNIL. In particular, the combination of (i) a description of processing, (ii) an assessment of necessity and proportionality, and (iii) a risk analysis followed by mitigation measures, is consistent with Article 35(7) GDPR and widely accepted good practice.

That said, there are several areas where the template could be further refined to enhance clarity, usability, and consistency in outcomes.

### **1. Structure and sequencing of information (Section 0 – Overview of the processing)**

The template introduces processors and sub-processors, including their respective roles, at an early stage (section 0.2), prior to a detailed description of the processing operations. While the intention to provide an overview of the actors involved in the processing is understandable, the sequencing appears conceptually inverted.

In practice, the identification and assessment of processors' roles, responsibilities, and risk profiles depend heavily on a clear understanding of the underlying processing operations. Without a sufficiently detailed mapping of the processing, including data flows, purposes, and technical architecture, the information provided on processors risks becoming formalistic rather than substantive.

This issue is particularly relevant in current operational contexts. A significant proportion of DPIAs are now triggered by vendor-driven solutions, where processors provide integrated, end-to-end services. In such cases, the processing logic is often largely predefined, and the controller's ability to meaningfully assess the role and impact of processors is contingent on first understanding how the processing operates in practice.

A revised structure could therefore prioritise a comprehensive description of the processing (including data flows and functionalities) before requiring a detailed characterisation of processors and sub-processors.

### **2. Absence of a defined or recommended risk methodology (Section 4.1 – Risk Assessment Method)**

The template requires controllers to describe the methodology used to assess risks, including likelihood and severity, but does not provide any baseline model or recommended approach.

While it is consistent with the GDPR's principle-based nature to avoid imposing a rigid methodology, the absence of even a non-binding reference framework represents a missed opportunity. Nearly a decade after the entry into application of the GDPR, DPIA practices remain highly heterogeneous, and methodological divergence continues to affect the comparability and reliability of outcomes.

Article 35(7)(c) GDPR requires an assessment of the risks to the rights and freedoms of natural persons, implicitly relying on the evaluation of likelihood and severity (as stated in article 32(1) GDPR). However, without a shared understanding of how these parameters should be interpreted and combined, different controllers may reach materially different conclusions when assessing comparable processing operations.

Experience in adjacent areas suggests that greater methodological convergence is both feasible and beneficial. For instance, structured approaches to personal data breach risk assessment have been developed, including by ENISA, and are complemented by guidance from the European Data Protection Board. Similarly, supervisory authorities have adopted more structured approaches in the calculation of administrative fines.

In both cases, the existence of methodologies has not eliminated contextual analysis but has contributed to reducing unnecessary variability.

Introducing a non-binding reference methodology, or at least illustrative models, would support greater consistency across DPIAs while preserving flexibility for controllers to adapt the approach to their specific context.

### **3. Usability and fragmentation of the description (Sections 1 and 2)**

The template adopts a highly structured format, breaking down the description of processing into multiple predefined fields. While this approach may facilitate standardisation, it also introduces a risk of fragmentation, particularly for complex processing operations.

In practice, controllers may find themselves describing the same elements across different sections with frequent cross-references (see the multiple references to points 1.1.a, 1.1.b and 1.1.c across the document). This can reduce readability, complicate internal review processes, and make the DPIA more difficult to maintain over time, especially when updates are required. For Controllers relying on GDPR Compliance software / SaaS, it might be challenging to materialise or replicate this structure.

A more balanced approach could combine structured fields with a narrative section that allows for a holistic description of the processing without losing the required level of detail. Such an approach would better reflect the reality of complex data processing activities and improve the overall coherence of the document.

### **4. Treatment of international data transfers (Section 4 – Necessity and Proportionality / Safeguards)**

While the template refers to safeguards for international transfers, the topic does not appear to receive a level of attention proportionate to its risk profile.

International data transfers, particularly to third countries without an adequacy decision, introduce a distinct layer of legal and operational risk. Following the Court of Justice's judgment in Schrems II, controllers are required to assess the effectiveness of transfer tools and, where necessary, implement supplementary measures.

Given these requirements, it would be beneficial for the template to include a more explicit and structured treatment of international transfers. This could involve dedicated prompts addressing transfer mechanisms, transfer impact assessments, and supplementary safeguards.

## 5. Consistency of outcomes and the role of DPIAs

A broader point relates to the function of DPIAs as instruments of risk management and protection of fundamental rights. While variability in outcomes is expected where factual circumstances differ, significant divergence in risk conclusions for comparable processing activities raises questions about the consistency of protection afforded to data subjects.

In contexts where processing operations are effectively standardised, such as vendor-provided solutions with limited scope for modification, methodological divergence may become a primary driver of differing outcomes. This could undermine the objective of ensuring a high and consistent level of protection across the Union.

Strengthening methodological guidance, even on a non-binding basis, would therefore contribute not only to consistency in compliance practices but also to the effectiveness of DPIAs as tools for safeguarding individuals' rights and freedoms.

## Final remarks

The EDPB's initiative to provide a DPIA template valuable. It establishes a common foundation and reflects widely accepted practices. The observations above are intended to support further refinement of the template, with a view to enhancing its practical usability and promoting greater consistency in its application.

In particular, adjustments to the structure, the introduction of non-binding methodological guidance, and a more explicit treatment of international transfers would significantly strengthen the template's contribution to effective risk assessment under the GDPR.

Diogo Duarte – 15/04/2026