Response to the public consultation on the EDPB DPIA Template

We have taken note of the European Data Protection Board (EDPB) Data Protection Impact Assessment (DPIA) Template which has been circulated for public consultation until 9th June, 2026. We are grateful for the opportunity to provide comments on the draft DPIA Template.

Areas of concern

We welcome the public consultation organised by the EDPB in relation to its DPIA Template and appreciate the opportunity to comment on it. The DPIA Template and its Explainer are important for organisations to help them to comply with the art. 35 GDPR requirements and are helpful in order to guide them how to conduct this process. However, it appears that the current DPIA Template is too complex and sophisticated for many organisations, especially for small and medium-sized enterprises (SMEs) that often need guidelines, which might cause a problem to complete it even with the Explainer provided.

Therefore, we would like to point out the following areas of concerns that will be elaborated later in our response:

1. Expansion beyond art. 35 GDPR requirements
    - Template goes significantly beyond the minimum legal DPIA requirements and normalises a highly formalised threshold for a DPIA to be properly conducted;
2. Lack of harmonised interpretation of high-risk processing across Member States
    - A single harmonised DPIA Template may be difficult to apply consistently across the EU in the absence of a common understanding among the 27 Member States of what constitutes “high-risk” processing requiring a DPIA;
3. Excessive administrative and documentation burden
    - Template prioritises traceability and repetitive documentation over practical privacy outcomes, creating unnecessary compliance complexity;
4. Limited practical applicability for SMEs and smaller controllers
    - The level of technical, organisational, and governance detail may be disproportionate and difficult for SMEs or less-resourced organisations to implement.

We therefore urge the EDPB to take into account these concerns and the suggestions hereunder and amend the DPAI Template.

1) Expansion beyond art. 35 GDPR requirements

A key concern relates to the extent to which the proposed DPIA Template appears to go beyond the minimum requirements established under art. 35 GDPR. While art. 35 GDPR requires controllers at minimum to describe the envisaged processing operations, assess necessity and proportionality, evaluate risks to the rights and freedoms of natural persons, and identify measures envisaged to address those risks, the proposed Template introduces a significantly broader set of operational, governance and documentation expectations. The accompanying Explainer further states that the Template represents *"a minimum amount of information that should always be documented"*, which suggests that, from the EDPB's perspective, a properly conducted DPIA should contain substantially more information than is at minimum required under the GDPR itself.

This also seems contrary to the approach presented in Guidelines on Data Protection Impact Assessment of the Article 29 Data Protection Working Party (WP29 Guidelines) - *"The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices"*.[1] The relationship between the Template and the WP29 Guidelines is not clearly explained, creating uncertainty for controllers regarding the threshold for compliance and the continuing role of the WP29 Guidelines as a benchmark for an adequate DPIA.

Additionally, the WP29 Guidelines state that a DPIA is generally required where two criteria are met, with a single criterion triggering a DPIA only in some cases[2]. The Template omits this qualification and might be read as suggesting that only one criterion is sufficient. The WP29 Guidelines also recognise that processing meeting one or more criteria may nevertheless not be likely to result in a high risk, provided the controller documents and justifies that assessment[3]. This flexibility is not reflected in the Template.

This raises important proportionality concerns, particularly in light of the GDPR's risk-based approach. The Template appears to normalise a highly formalised threshold as the expected baseline for all DPIAs, regardless of the nature, scale, complexity or actual level of risk associated with the processing operation. In particular, the Template includes extensive requirements relating to, among others, version logs and DPIA lifecycle tracking, architectural and asset inventories or detailed action plans. While such elements may constitute valuable best practices for particularly high-risk, large-scale or technically complex processing operations, they may not always be necessary or proportionate for moderate-risk processing activities, SMEs or controllers with limited legal and technical resources.

The repeated emphasis throughout the Template and Explainer on extensive documentation, structured methodologies and formal governance processes also raises the question whether the proposed framework fully reflects the GDPR principles of proportionality.

[1] WP29 Guidelines (wp248rev.01), p.17.
[2] WP29 Guidelines (wp248rev.01), p. 11.
[3] WP29 Guidelines (wp248rev.01), p. 12.

In this context, the Template would benefit from a clearer distinction between mandatory art. 35 GDPR requirements, recommended best practices and enhanced expectations applicable only in specific high-risk or large-scale processing contexts. A more modular or scalable approach could better reflect the GDPR's proportionality principle and improve the practical usability of the Template, particularly for SMEs and lower-risk processing operations. Certain expectations could also be identified more explicitly as optional or context-dependent, rather than being presented as universally applicable minimum requirements.

2) Lack of harmonised interpretation of high-risk processing across Member States

The objective of creating a common and harmonised DPIA framework is welcomed and would in principle provide greater legal certainty for organisations operating across multiple Member States. However, the usefulness of a single template remains limited in the absence of a harmonised understanding of when a DPIA is actually required.

Under art. 35(4) GDPR, several national data protection authorities (DPAs) have published lists of processing operations that are considered likely to result in a high risk and therefore require a DPIA. Such lists have been adopted, among others, by the DPAs in France, Belgium, Germany, Spain, Italy and Poland. Currently there are significant divergences existing between Member States regarding the interpretation of "high-risk" processing and the thresholds triggering a DPIA obligation.

In this context, it is difficult to assess how a single harmonised template can be effectively and consistently applied across all 27 Member States when there is still no fully harmonised assessment methodology for determining whether a DPIA is required in the first place. The current approach risks creating a highly detailed and burdensome template without first addressing the more fundamental issue of legal certainty concerning the scope of the DPIA obligation.

In this regard, the ongoing discussions within the Digital Omnibus proposal to amend art. 35 GDPR is particularly relevant. The proposed amendments foresee that the EDPB would prepare and transmit to the Commission proposals for harmonised lists of processing operations requiring or exempt from DPIAs, as well as a common template and common methodology for conducting DPIAs. This approach is welcomed and could significantly improve consistency and legal certainty across the Union. However, such harmonisation should reflect an existing and clearly established consensus among DPAs rather than lead to an expansion of DPIA obligations beyond what is currently required at national level. Any common methodology or harmonised list should therefore remain proportionate and risk-based.

Furthermore, consideration should also be given to legal certainty for organisations that have already implemented processing operations in compliance with existing national guidance. In this respect, it would be useful to clarify that any newly harmonised DPIA requirements or methodologies would apply prospectively to new processing operations and should not trigger

retroactive reassessments of existing processing activities already considered compliant under current national frameworks.

It would be therefore very useful for the EDPB to consider creating and prioritising the development of a unified decision tree or common assessment methodology, valid across all Member States, to assist organisations in determining when processing activities are likely to present a “high risk” under art. 35 GDPR and therefore require a DPIA. Such guidance would significantly improve consistency, predictability and harmonisation across the EU before introducing a detailed common template.

3) Excessive administrative and documentation burden

A further concern relates to the significant administrative and documentation burden that may result from the proposed DPIA Template and accompanying Explainer. Both documents place a strong emphasis on traceability and completeness, with the Explainer expressly acknowledging that redundancy between sections is intentional. In practice, this may require controllers to repeat similar analyses, safeguards and mitigation measures across multiple sections, including compliance, security and residual-risk tables, without necessarily improving substantive privacy outcomes.

As a result, there is a risk that the DPIA process may become overly formalistic, with the completeness of documentation taking precedence over the substantive quality of the risk assessment itself. This could create a significant administrative burden without necessarily improving the protection of individuals’ rights and freedoms.

In addition, section 1.1.c of the EDPB Template requires controllers to provide information on any secondary or compatible uses of the data involved in the processing. However, at the time an initial DPIA is conducted, such secondary purposes and any related compatibility assessments may not yet be identified. Without further clarification, some controllers may interpret this requirement as obliging them to anticipate and assess all potential future uses of the data, even where no such uses are currently envisaged. To avoid this misunderstanding and better reflect practical realities, the EDPB could clarify that this information should be provided only where such secondary or compatible uses are known, for example by adding the qualifier “if known” to this section of the Template.

Moreover, section 2.2.b of the EDPB Template requires controllers to provide information on “data quality,” including “quality metrics, requirements or thresholds.” However, neither the Template nor the Explainer clarifies what type of information is expected under this heading or how it contributes to the DPIA assessment. In the absence of further guidance, controllers may face uncertainty as to how to complete this section, potentially resulting in unnecessary complexity and administrative burden.

The highly documentation-heavy approach also appears difficult to reconcile with the current broader EU objectives aimed at simplifying digital regulation and reducing unnecessary administrative burdens, including recent initiatives concerning the simplification of the GDPR. As a consequence, the Template may contribute to increased compliance complexity rather than facilitating practical and accessible DPIA implementation across organisations of different sizes and risk profiles.

4) Limited practical applicability for SMEs and smaller controllers

The combined documents repeatedly emphasise extensive documentation, structured methodologies and formal governance processes, while the GDPR itself is intended to operate on the basis of proportionality, scalability and a risk-based approach. Although the Template may be well suited for large-scale, high-risk or technically complex processing operations, its overall level of detail and operational expectations may prove disproportionate for SMEs, lower-risk controllers or organisations carrying out limited-scope processing activities.

In practice, smaller organisations often operate with significantly more limited legal, technical and compliance resources than larger enterprises. The level of granularity required throughout the Template, together with the extensive governance and documentation expectations, may therefore create substantial practical difficulties in completing and maintaining the DPIA process. As a result, the Template risks increasing the complexity and administrative burden of GDPR compliance rather than facilitating practical implementation.

The concern is not that the additional elements included in the Template are inherently inappropriate or without value. Many of the proposed governance, documentation and technical assessment measures may constitute useful best practices for particularly high-risk processing activities. However, the current structure of the Template appears to present these expectations as broadly applicable minimum standards, rather than measures that should be adapted to the specific context, scale and level of risk of the processing operation.

The objective of the Template is clearly to support organisations in complying with the GDPR and to promote greater consistency in conducting DPIAs across the European Union. However, due to its complexity and level of detail, the Template may not fully achieve this objective in practice, even with the additional guidance provided in the Explainer.

***

We thank you in advance for taking into consideration these concerns and suggestions to ensure that this public consultation leads to meaningful changes to the DPIA Template.