bitkom

Position Paper

2026 June

Bitkom on the EDPB´s Template for Data Protection Impact Assessment

Summary

Bitkom welcomes the EDPB's objective of enhancing consistency in how DPIAs are conducted across the EU, as well as the initiative to provide standardised templates to facilitate the application of the GDPR.

However, Bitkom argues that the current draft template goes beyond the legal requirements of Article 35(7) GDPR. Instead of focusing solely on assessing risks to individuals' rights and freedoms, the template includes additional normative requirements and best practices without clearly distinguishing them from the mandatory elements of a DPIA. As a result, it expands significantly beyond the four required DPIA components:

- Description of the processing activities
- Assessment of necessity and proportionality
- Assessment of risk to rights and freedoms
- Measures to address those risks

While supporting practical guidance and standardisation that help organisations in identifying, assessing, and mitigating risks to data subjects, Bitkom encourages the EDPB to ensure that the final template remains proportionate, practical, and focused on the requirements of Article 35 GDPR. We suggest that the current proposal may create unnecessary administrative burdens and could require organisations to provide sensitive technical and operational information that is not typically required for a DPIA. The template should be designed to meet the requirements of all EU Member States and should remain proportionate for processing operations presenting different levels of risk, including lower-risk operations that still occur in practice. To improve usability and consistency, Bitkom also recommends including a clear checklist or tick-box format in the final template.

Misalignment with Article 35 GDPR

The draft template goes beyond the legal requirements set out in Article 35(7) GDPR and transforms the DPIA into a broader compliance and documentation exercise.

- The template introduces elements such as detailed principle-by-principle compliance mapping, implementation status tracking, and extensive documentation of measures across multiple categories.
- It embeds references to non-binding guidance (e.g. EDPB/EDPS guidelines) without clearly distinguishing between legal obligations and best practices.
- It includes requirements such as formalised risk staging (inherent vs. residual risk) and implementation tracking that relate more to compliance maturity than to risk assessment.

This creates legal uncertainty. If the template is intended as best practice, elements exceeding Article 35 GDPR should be clearly identified as optional. If it is intended as a benchmark for supervisory authorities, it must remain strictly within the legal scope of Article 35 GDPR.

The template should therefore not inadvertently lead to DPIAs becoming overly prescriptive, technical, contractual, or containing operational catalogues beyond what Article 35 GDPR requires.

Disproportionate Level of Detail and Administrative Burden

The template imposes a level of granularity that is disproportionate to the purposes of a DPIA as a risk – based tool. Extensive documentation requirements risk shifting focus away from substantive risk analysis toward formalistic completion of template fields. Furthermore controllers, particularly small and medium sized organisations, may struggle to meet the required level of detail for each DPIA. In complex processing environments the template requires information that is difficult to obtain or duplicate.

This creates a risk of formalistic compliance, or, alternatively, disproportionate resource allocation without corresponding benefits for data subjects.

In addition, the template may require organisations to disclose sensitive technical and operational information that is not necessary for a DPIA under current practice.

Lack of Risk – Based Flexibility

The template does not sufficiently reflect the risk-based nature of Article 35 GDPR. It applies a uniform structure and level of detail regardless of the nature, scope, or risk profile of the processing. It requires completion of sections that may not be relevant,

e.g. automated decision-making safeguards where no such processing exists. The rigid tabular format limits the ability to carry out and document nuanced balancing of interests.

A DPIA should be adaptable to the specific context of the processing. The template should therefore:

- Clearly distinguish between mandatory and optional sections
- Allow for a proportionate depth of analysis
- Provide more flexibility in format (including free-text elements)

Conflation of DPIA with General Compliance Documentation

The draft template treats the DPIA as a self-contained compliance instrument, requiring controllers to reproduce documentation and verification that the GDPR's accountability framework assigns to other mechanisms, such as Art. 30 GDPR (records of processing activities), Art. 28 GDPR (processor agreements), and Articles 40 and 42 GDPR (codes of conduct and certifications).

This approach fundamentally conflates two distinct functions: risk assessment under Art. 35 GDPR and general compliance documentation under the accountability principle. A DPIA is intended to assess whether a specific processing operation is likely to result in high risks to the rights and freedoms of natural persons and to identify measures to mitigate those risks. It is not designed to serve as a comprehensive inventory of processing activities, nor as a full compliance audit. By merging these functions, the template risks diluting the analytical core of the DPIA and shifting the focus towards formalistic documentation.

This conflation is reflected throughout the structure of the template:

- **Section 1** requires a highly granular breakdown of the processing operation, including detailed sub-categories such as data types, purposes, operations, scope, context, data lifecycle, technical means, and supporting assets. This level of detail mirrors the structure of Art. 30 GDPR records rather than the »systematic description« required under Art. 35(7)(a) GDPR, and risks duplicating existing documentation without adding value to the risk assessment.
- **Section 2.2.b** introduces requirements such as data quality metrics per data category. While relevant in a broader data governance context, such metrics are not inherently linked to the assessment of risks to data subjects and therefore fall outside the core purpose of a DPIA in many cases. We recommend that the term »data quality« should be removed as it is not directly relevant under the GDPR, and that Section 2.2.b should therefore be deleted.
- **Section 2.3** requires extensive documentation of compliance measures across multiple dimensions, including GDPR principles, data subject rights, processor and transfer obligations, data protection by design, and security measures. Each element

must be accompanied by a discussion of appropriateness and effectiveness. This effectively turns the DPIA into a comprehensive accountability checklist rather than a targeted risk analysis.

- The mandatory implementation status labelling (e.g. »planned«, »partially implemented«, »implemented«) further reinforces this shift. Such categorisation reflects compliance maturity and implementation progress, not the existence or severity of risks to data subjects. As a result, the assessment risks becoming detached from its primary objective of evaluating and mitigating risk.

These issues are particularly pronounced in cloud-based and outsourced processing environments. The template requires detailed documentation of infrastructure components (e.g. servers, storage media, VPN gateways, data centres) and associated security measures, without adequately accounting for the shared responsibility model. Controllers relying on cloud providers typically achieve a high level of security through contractual arrangements, certifications, and standardised controls. However, the template does not provide a mechanism to recognise or rely on such evidence. This creates a structural disadvantage for cloud-based controllers, who must either duplicate provider-level documentation or leave sections artificially incomplete, despite benefiting from robust security frameworks.

More broadly, the template operates as if each DPIA exists in isolation, disregarding the reality that most organisations implement integrated compliance frameworks. Requirements to re-document security measures, processor safeguards, and transfer mechanisms within each DPIA ignore the role of existing tools such as certifications, audit reports, and standard contractual arrangements. Articles 28(5) and 42 GDPR explicitly recognise certifications as valid means of demonstrating compliance, yet the template does not allow for meaningful reliance on such mechanisms through cross-references.

Further examples of this misalignment include:

- **Section 4.2.c**, which requires a detailed action plan including responsibilities, timelines, and monitoring mechanisms. While useful for internal governance, this goes beyond Article 35(7)(d) GDPR, which only requires the identification of measures envisaged to address risks. In practice, implementation tracking is typically managed through separate project management or compliance systems, often by different organisational functions.

- **Explainer 0.5 technical sheet:** The Explainer requires »"approval of the DPIA as complete and finished by a responsible official (Managing Director, CEO, etc.) «, imposing a C-suite sign-off gate for every DPIA. Article 35 GDPR contains no such requirement. DPIAs are typically coordinated by privacy and legal functions, while executive sign-off sits with a different governance layer, creating cross-functional friction without improving assessment quality. Rather than requiring sign-off by local management, the template could provide that the local DPO should be involved on a mandatory basis. The DPO may then report residual risks to management and escalate where appropriate. This could offer a more proportionate solution while remaining consistent with the GDPR framework.

We consider it important that management is appropriately informed about residual risks and is able to take them into account in a deliberate manner. However, regular top management sign-off may not be necessary in all cases, in particular in group structures where DPIAs are conducted on a group-wide basis while compliance risks remain primarily local. In this context, best practice guidance on how to document data protection risks in a structured way would be helpful, so that they can be appropriately reflected in management reporting without requiring mandatory periodic approval by top management. A clarification from the EDPB on this point would be particularly helpful. Overall, the cumulative effect of these elements is to transform the DPIA from a focused risk assessment tool into a hybrid instrument combining elements of compliance documentation, audit, and governance reporting. These risks overburdening controllers, duplicating existing processes, and ultimately reducing the effectiveness of DPIAs as tools for identifying and mitigating risks to individuals.

The template should therefore be revised to clearly separate risk assessment from general compliance documentation. In particular, it should:

- Focus on the core elements required under Article 35(7) GDPR.
- Allow and encourage references to existing documentation and compliance mechanisms rather than duplication.
- Avoid introducing additional governance, reporting, or project management requirements.
- Ensure that all required elements directly contribute to the assessment of risks to data subjects and the identification of appropriate mitigation measures.

Structural and Methodological Issues in Specific Sections

Several parts of the template raise specific concerns regarding clarity, usefulness, and internal consistency:

- **Security measures (Section 2.3.e): The** assessment of technical and organisational measures is required without a clear link to specific risks, contrary to Article 32 GDPR. The structure is unclear and risks inconsistent application. This section should be removed or integrated into the risk assessment sections.
- **Data subject rights (Section 2.3.b):** Grouping different rights (e.g. rectification and erasure) in a single line reduces clarity and may obscure gaps in implementation. These rights should be assessed separately.
- **Use of terminology:** The introduction of «legal/contractual measures» alongside technical and organisational measures deviates from established GDPR terminology and should be avoided.
- **Processor assessment:** The template does not adequately support a meaningful, risk-based assessment of processors and may lead to incomplete or inconsistent documentation.
- **Data processor and sub-processor details (Section 0.2- Explainer):** Data processor and sub-processor details should be risk-relevant, not exhaustive or redundant with existing GDPR obligations such as Article 28. The Template DPIA should not require detailed listing of sub-processors, and contractual tasks already addressed through Article 28 of the GDPR.
- **Scope of the DPIA (Section 0.5- Explainer)**: The scope of the DPIA should focus on the processing being carried out that is covered by the DPIA. The Template DPIA should only address what is not considered where this is relevant to assessing the necessity of the DPIA. Requiring the documentation of processing that is not covered in the DPIA, and why it is not covered, risks creating an unnecessary inventory of features, configurations, integrations and deployment choices that are outside a particular use case without added value. It is also not prescribed by the GDPR.
- **Publication or external sharing (Section 0.5-Explainer):** Publication or external sharing of the DPIA should be discretionary. The Template DPIA should not imply that its publication or external sharing is expected, because DPIAs may contain confidential information about controls, infrastructure, risk assumptions, mitigation strategies, contractual arrangements, system architecture and operational dependencies.

Architecture and supporting assets (Section 1.3): Architecture and supporting assets should be described at the appropriate level of detail. The Template DPIA should not require granular or exhaustive infrastructure details such as asset-level hardware, network components, software modules, technical layers or functions. Requiring that

level of detail may be unnecessary for the DPIA and may raise security or confidentiality concerns.

Format and Usability Limitations

The use of a static Word-based template limits the practical usability of the DPIA and increases the risk of inconsistencies and omissions, particularly in more complex processing scenarios. The format does not support basic functionalities such as automated consistency checks or structured linking between sections, which are essential for ensuring completeness and coherence. It also does not enable graphical representations of processing activities, despite their recognised value for understanding data flows and identifying risks. We suggest that the template should work with clear tick-boxes to improve usability and ensure consistency. In addition, the provision of a RACI matrix, to clarify roles and responsibilities could be helpful, rather than requiring companies to develop this themselves.

In practice, these limitations may lead to inefficiencies and reduce the quality of assessments. Experience with existing tools, such as the CNIL's PIA software, shows that digital solutions can significantly improve usability, reduce errors, and increase adoption. The EDPB may therefore wish to consider supporting or exploring the development of a complementary software-based approach that better reflects how DPIAs are carried out in practice.

Accessibility and Need for Enhanced Guidance

The template assumes a level of data protection expertise that limits its accessibility, particularly for organisations without specialised privacy resources. Key concepts, such as the GDPR principles, are not explained, and there is a lack of practical examples to guide users in applying them. As a result, the template may be difficult to use effectively, especially for smaller organisations.

To improve usability and acceptance, the accompanying explainer should be expanded to include clearer explanations and practical examples. More interactive or digital guidance could further support users by providing contextual assistance and making the assessment process more intuitive.

Missed Opportunity for Regulatory Alignment

The template does not sufficiently reflect overlaps with other regulatory frameworks, in particular the AI Act. DPIAs and Fundamental Rights Impact Assessments share key elements, and in many cases will apply to the same processing activities. The absence of alignment risks creating duplicative assessments and unnecessary administrative burdens.

The template should therefore be designed to facilitate interoperability, allowing controllers to reuse DPIA elements where regulatory requirements overlap.

Recognising DPIAs as a potential basis for fulfilling related obligations would contribute to greater coherence and reduce duplication in an increasingly complex regulatory landscape.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Elena Kouremenou | Policy Officer for Data Protection
P +49 30 27576-425 | e.kouremenou@bitkom.org

Isabelle Stroot | Head of Data Protection Law and Policy
P +49 30 27576-228 | i.stroot@bitkom.org

Responsible Bitkom committee
WG Data Protection