MedTech Europe Response to the EDPB Public Consultation on DPIA Template

June 2026

Introduction

MedTech Europe appreciates the opportunity to provide input on the draft European Data Protection Board's (EDPB) Data Protection Impact Assessment (DPIA) template.

As a European trade association representing the medical technology industry, we support initiatives that promote consistent and high-quality data protection practices across the EU. We recognise that a structured template may provide useful guidance, particularly for organisations with limited experience in conducting DPIAs or resources.

At the same time, more than eight years after the application of the General Data Protection Regulation (GDPR),[1] organisations in our sector have already developed mature, risk-based DPIA frameworks and internal tools, integrated into broader compliance and risk management systems. In this context, it is essential to ensure that the introduction of a new template does not create unintended compliance expectations or disrupt well-functioning existing approaches, but instead remains a flexible and supportive tool.

Key considerations and challenges

i. Risk of a de facto mandatory template

A primary concern for the medical technology industry is the risk that the template could, in practice, be perceived or applied as a standardised format for DPIAs. In the absence of explicit clarification, organisations may face uncertainty as to whether supervisory authorities will expect DPIAs to follow the proposed structure or may challenge or discount DPIAs presented in alternative formats. Such uncertainty may create additional compliance burden without improving data protection outcomes.

ii. Misalignment with existing mature practices

More broadly, the template does not sufficiently reflect the reality that many organisations already operate established DPIA methodologies tailored to their specific business models and organisational structures. In the medical technology sector, companies often function across multiple jurisdictions, rely on integrated compliance tools, and apply risk-based methodologies designed to address complex and evolving processing activities. Encouraging the use of a uniform and highly detailed template risks undermining these mature systems without clear added value.

iii. Complexity and lack of proportionality

The level of detail and granularity of the template also raises concerns from a proportionality perspective. While such detail may provide useful structure in certain contexts, the extensive documentation requirements may be difficult to apply in practice, particularly for organisations conducting multiple DPIAs across diverse activities. There is a risk that this approach could encourage formalistic or "tick-box" exercises, rather than fostering meaningful and outcome-oriented risk assessments, which are at the core of Article 35 GDPR.

This approach may also run counter to broader EU policy objectives, including ongoing efforts to simplify regulatory requirements and reduce administrative burden, as reflected in initiatives such as the Digital Omnibus.

[1] Regulation (EU) 2016/679, available here.

iv. Limited usability in operational contexts

From an operational perspective, the usability of the template presents additional challenges. DPIAs in the medical technology sector typically involve input from a wide range of stakeholders, including legal, compliance, IT, clinical and R&D functions. The structure and complexity of the template may limit its accessibility for non-legal stakeholders and may not align with existing workflows, particularly in large multinational organisations where responsibilities are distributed.

Certain assumptions embedded in the template also appear to reflect simplified organisation models and may not be compatible with governance structures in large, multinational organisations.

v. Lack of guidance on methodology and lifecycle

The template also provides limited guidance on key methodological aspects. In particular, while organisations are expected to define their own risk assessment approaches, no reference methodology or practical examples are provided. This creates practical challenges, as organisations lack concrete examples or reference approaches to assess risks in a consistent and meaningful way. This may lead to divergent interpretations and inconsistent outcomes across organisations.

Similarly, the template does not offer sufficient clarity regarding the lifecycle of DPIAs, including when and how they should be updated in the context of evolving processing activities such as software iterations, clinical investigations or post-market monitoring.

More broadly, while we recognise that this initiative focuses on a DPIA template, it also highlights the continued lack of harmonised criteria at EU level regarding when a DPIA is required. Divergences across Member States, including through national lists of processing operations requiring a DPIA, create legal uncertainty and additional compliance burden for organisations operating cross-border.

vi. Structural and conceptual issues

Certain structural aspects of the template could also benefit from refinement. For example, the separation of data protection by design and by default from other compliance elements may duplicate concepts already embedded across the assessment. In addition, the sequencing of certain sections does not fully reflect how DPIAs are typically conducted in practice, where the need for a DPIA is often determined following an initial assessment of the processing.

vii. Insufficient consideration of sector-specific realities

Finally, the template remains highly generic and does not adequately reflect sector-specific realities. In particular, there is limited practical consideration of the processing of special categories of personal data, despite their central importance in healthcare and medical innovation. The absence of sector-specific examples reduces the practical relevance of the template for organisations operating in complex and highly regulated environments such as the medical technology sector.

Our recommendations

In light of the above, MedTech Europe recommends that the EDPB:

- Clearly confirm that the DPIA template is **entirely optional**, and that organisations are not required to adopt it or align existing DPIAs with its structure;
- Clarify that **compliance will be assessed on the basis of substance rather than format**, and that supervisory authorities will not use the template as a benchmark;
- Ensure that the template is positioned as a **flexible and illustrative tool**, which complements rather than replaces existing DPIA frameworks;
- Strengthen the emphasis on **proportionality and risk-based application**, reflecting the diversity of processing activities and organisational models;
- Improve the **usability and flexibility**, allowing for more modular and adaptable approaches aligned with operational realities;

- Provide **practical guidance and examples**, including illustrative DPIAs and reference risk assessment methodologies;
- Clarify expectations regarding the **lifecycle and updating of DPIAs**, particularly for evolving and long-term processing activities;
- Consider the development of **sector-specific guidance or use cases**, including for the processing of health data and activities typical of the medical technology sector.

Conclusion

MedTech Europe supports the objective of promoting robust and consistent DPIA practices across the EU. However, in the current context, the introduction of a detailed DPIA template should be carefully calibrated to avoid unintended consequences. It is essential that any such template remains non-prescriptive, proportionate and fully aligned with existing practices, ensuring that it supports organisations without introducing unnecessary complexity or legal uncertainty.

In addition, we encourage the EDPB to ensure that further work in this area is consistent with broader EU policy objectives on simplification, reduction of administrative burden and support for innovation. This is particularly important for sectors such as medical technology, where data-driven innovation plays a critical role in improving patient outcomes and supporting sustainable healthcare systems.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.
www.medtecheurope.org.

For more information, please contact:

Mirella Kavadaki
Manager Legal & Compliance – Legal Counsel
MedTech Europe
m.kavadaki@medtecheurope.org