CEDPO Contribution on the EDPB Draft DPIA Template

Public consultation response

CEDPO welcomes the EDPB's initiative to provide a common DPIA template intended to improve consistency, completeness and usability across the European Economic Area.

A common structure can help controllers document their assessments more clearly, support internal governance and facilitate more predictable supervisory expectations.

At the same time, the practical value of any DPIA template depends less on the form itself than on the quality of the underlying analysis, the proportionality of the documentation expected and the clarity of the governance surrounding the process.

General remarks

CEDPO supports the objective of creating a practical and harmonised reference framework for DPIAs. The draft is comprehensive and usefully covers the main stages of the exercise, from the description of the processing to the assessment of necessity, proportionality, risks, mitigation measures, consultation and final decision-making.

However, a template will only improve compliance if it is understandable and workable for the organisations expected to use it in practice. The draft would therefore benefit from further clarification on governance, methodology, proportionality and the circumstances in which an existing DPIA should be updated or replaced.

CEDPO also considers that the final template should remain capable of being used as an adaptable reference model rather than being perceived as a mandatory one-size-fits-all reporting form. This is important to preserve its usefulness for organisations of different sizes, sectors and maturity levels, and to ensure compatibility with existing national practices and risk assessment frameworks.

1. The role of expertise in producing a meaningful DPIA

A well-drafted DPIA requires more than the completion of predefined fields. Its quality depends on the involvement of persons with sufficient knowledge of data protection law, risk assessment and, where relevant, information security, system design, product, operational and business processes.

The template would benefit from clearer wording in the introductory material or explanatory guidance stating that a DPIA should be prepared with appropriate multidisciplinary input, and that organisations should ensure access to suitable expertise when assessing necessity, proportionality, risks and mitigating measures.

This point is especially important for organisations that may otherwise treat the exercise as a documentation formality rather than a substantive accountability process. It would also help avoid the practical misconception that the DPO alone is expected to produce the DPIA, rather than advise and support a process owned by the controller.

2. Clarifying the role of the DPO

Section 5.1 rightly requires the DPO's advice to be recorded. However, the template should more clearly distinguish between the role of the controller, who remains responsible for the assessment and the decisions taken, and the role of the DPO, whose function is to advise and monitor compliance.

In particular, the template should make explicit that the controller may decide not to follow the DPO's advice, but that any such decision should be documented together with the reasons for doing so. This is important both for accountability purposes and to avoid any misunderstanding that the DPO is the decision-maker for the DPIA or bears responsibility for the controller's final choices.

CEDPO also suggests that the relevant field in section 5.1 should allow sufficient space for meaningful explanations, while avoiding overly formalistic requirements. The template should capture whether the DPO raised reservations, whether those reservations were addressed and how the controller ultimately resolved them, without turning the consultation section into a disproportionate administrative exercise.

3. Proportionality and operational usability

The template is detailed and structured, which is valuable for harmonisation. Nevertheless, it should not be perceived primarily as a legal reporting instrument. DPIAs are most effective when they can be used by business, product, technical, security and operational teams, with the support of privacy professionals, to identify and reduce risks in practice.

CEDPO therefore recommends that the EDPB include guidance on how the level of detail expected in the template may be calibrated to the nature, scope, context and purposes of the processing and to the severity and likelihood of the risks involved. This could be achieved by distinguishing core information expected in most DPIAs from enhanced prompts that are relevant only for more complex or higher-risk processing operations.

This proportional approach would be particularly useful for fields that can otherwise become very burdensome without necessarily improving the analysis. For example, where processors and sub-processors are described, it may often be sufficient to identify their role, the categories of tasks entrusted to them and the existence of Article 28 GDPR arrangements, rather than requiring a detailed repetition of all contractual obligations in the DPIA itself.

Similarly, action plans should focus on the additional measure, the responsible function or owner, the expected timeframe and the effect on residual risk. Further administrative detail should remain optional where it is not necessary for accountability or risk management.

4. Improving the methodology and flow of the template

The distinction between section 3.1, which addresses impacts on the rights and freedoms of data subjects, and section 4.1.a, which concerns impacts caused by non-default, accidental, unlawful or abnormal events, may not be immediately clear to many users. Although this distinction may be intelligible to experienced privacy professionals, it risks being perceived by business teams and specialist departments as redundant or unnecessarily complex.

The sequencing of the template also deserves reconsideration. From a practical standpoint, some users may find it counterintuitive to address impacts in section 3.1 before completing the analysis of necessity and proportionality in sections 3.2 and 3.3.

Additional drafting guidance, or a short explanation of the logic behind this structure, would significantly improve usability without changing the substance of the template. In particular, the EDPB should clarify how impacts, threats, necessity, proportionality and risk management interact, and when the same information should not be repeated in several sections.

The identification of secondary purposes is relevant, particularly in the context of data re-use. However, the template should make clear how foreseeable secondary purposes should be documented without requiring controllers to anticipate purely speculative uses. Likewise, the section dealing with data quality would benefit from a clearer explanation of its intended meaning and practical examples.

5. Risk assessment and security concepts

Where security, architecture or operational resilience are relevant to the assessment, the contribution of information security or equivalent technical functions should be expressly encouraged.

CEDPO also suggests that the template should remain compatible with established security risk assessment practices. In particular, where relevant, it should allow controllers to distinguish between risks relating to confidentiality, integrity and availability, even if the final DPIA presents an overall consolidated risk analysis.

This clarification would help organisations connect the DPIA to existing security frameworks and avoid unnecessary rework. It would also make the template easier to use in organisations where security risks are already assessed through structured methodologies that distinguish between these dimensions.

6. AI-related processing

CEDPO recommends adding a proportionate prompt or short section on AI-related processing. AI-enabled systems increasingly form part of processing operations that may require a DPIA, including profiling, decision support, automated inference, generative AI use cases and the training, tuning or monitoring of models.

The objective should not be to turn the DPIA template into a comprehensive AI Act compliance checklist. Rather, the template should help controllers identify, where relevant, whether AI-related features affect the assessment of necessity, proportionality, data minimisation, transparency, human oversight, accuracy, bias, data quality, security, explainability or risks to individuals.

Such a prompt should apply in a risk-based and proportionate manner. Where a use case also falls within the scope of specific AI legislation, the DPIA could cross-refer to the relevant assessment or documentation, instead of duplicating it.

7. Reconsidering certain structural choices and review triggers

The draft includes a separate section on measures supporting data protection by design and by default. While the principle itself is clearly important, some users may question whether this part adds a distinct analytical step or instead duplicates matters already covered by the preceding sections on lawfulness, minimisation, compliance measures and security.

The EDPB may therefore wish to clarify the intended function of this section. If the objective is to identify additional design choices not already captured elsewhere, that should be stated expressly. If not, the analysis could be integrated more clearly into the preceding compliance sections in order to reduce duplication and improve readability.

CEDPO also notes that the questions concerning the reasons for conducting the DPIA could arguably sit later in the overall logic of the document, once the core description and analysis of the envisaged processing have been completed. Even if the current structure is maintained, the explanatory material should make clearer whether all sections are expected to be completed for each new processing operation and at what point the dedicated risk management section becomes necessary in practice.

The draft already contains elements relating to version history, planning and the reasons for conducting the DPIA, including situations where an existing high-risk processing activity has changed. Nevertheless, the template would benefit from a more explicit and operational section addressing when a DPIA must be reviewed, updated or conducted again.

In particular, the EDPB should consider adding a dedicated prompt on review triggers, such as changes to the purposes of the processing, the means used, the legal basis, categories of personal data, data recipients, international transfers, the use of AI-related features or the overall risk profile of the processing.

Proposed amendments

- Clarify in section 5.1 and in the explanatory material that the DPO provides advice, but the controller remains responsible for decisions taken.
- Add an explicit field requiring the controller to document any decision not to follow the DPO's advice, together with the reasons for that decision.
- State more clearly that DPIAs should be prepared with appropriate multidisciplinary input, including business, technical and security functions where relevant.
- Provide guidance on proportionality, including which fields are core and which should be completed only where relevant to the complexity or risk level of the processing.
- Explain more clearly the distinction between the impacts considered in section 3.1 and the event-driven risks addressed in section 4.1.a.
- Clarify the intended methodological flow between impacts, threats, necessity, proportionality and risk management.
- Clarify how secondary purposes and data quality should be documented, preferably with practical examples.
- Allow the risk assessment to distinguish between confidentiality, integrity and availability where this is useful or consistent with the organisation's security methodology.
- Reassess whether section 2.3.d adds distinct value as a standalone section, or clarify how it differs from other compliance-oriented sections.
- Provide more operational guidance on whether all sections are meant to be completed for every new processing operation and when the dedicated risk management section should be activated in practice.
- Add a specific section or prompt on review triggers and the circumstances requiring an update or a new DPIA.
- Add a concise, risk-based prompt on AI-related processing, without duplicating AI Act compliance documentation.
- Improve usability by avoiding unnecessary duplication and allowing the use of narrative text rather than tables where tables are not the most appropriate format.

Closing observation

CEDPO supports the adoption of a common EDPB DPIA template and considers that the current draft provides a strong basis for greater consistency across Europe.

The adjustments suggested above are intended to strengthen the template's practical usefulness, preserve the distinction of roles within the GDPR accountability framework and ensure that the document supports substantive, proportionate and operational risk assessment rather than formal completion alone.