DOT Europe consultation response

EDPB DPIA Template

Introduction

DOT Europe welcomes the opportunity to comment on the EDPB's draft template for Data Protection Impact Assessments (DPIA).

Before turning to the substance of our recommendations, we would like to highlight an overarching consideration regarding the current Digital Omnibus process, specifically on the proposed amendments to Article 35 GDPR. In line with the EDPB/EDPS Joint Opinion on the Digital Omnibus, we welcome the proposed changes, in particular the development of a common template and methodology for conducting Data Protection Impact Assessments. The proposal introduces positive measures aimed at improving legal clarity and harmonisation across the EU, including through the establishment of EU-wide "black" and "white" lists of processing operations.

We recognise that the aim of the DPIA template is to assist smaller enterprises who may not have existing dedicated data protection resources or sophisticated compliance frameworks. At the same time, the DPIA template should remain voluntary in order to preserve flexibility for organisations that already have effective and well-established frameworks in place, and to avoid creating unnecessary administrative burdens. Such a voluntary character will also avoid that harmonised DPIA requirements from leading to retroactive obligations or compliance burdens without any added value.

Overarching Concerns

The EDPB template appears to depart from the flexible approach to DPIAs reflected in the WP248rev.01 guidance ("WP29 Guidance"). The WP29 Guidance explains that the GDPR allows controllers flexibility in determining the structure and format of a DPIA so that it can align with existing organizational practices. By contrast, the EDPB template's "Explainer" indicates that the template is intended to capture "a minimum amount of information that should always be documented" in DPIAs, while also providing a level of detail that goes beyond the considerations identified in the WP29 Guidance for assessing whether a DPIA is sufficiently comprehensive under the GDPR.

In addition, the template generally does not distinguish between mandatory and optional information, nor does it indicate where a more limited level of detail may be appropriate. As a result, controllers may reasonably interpret the template as establishing an expectation that all fields be completed in order for a DPIA to be considered adequate.

This risks shifting the DPIA process toward a more prescriptive and burdensome approach than that contemplated by the GDPR and prior guidance.

A related concern runs across several sections: the template embeds obligations from non-binding EDPB/EDPS guidance, such as the EDPS Necessity Toolkit, EDPB Guidelines on Art. 6(1)(f), and Guidelines on Art. 25 via footnote references and mandatory fields, without distinguishing these from statutory requirements.

Furthermore, across multiple sections, the template creates duplication with documentation obligations that are already established under other provisions of the GDPR or other regulatory frameworks: sub-processor listings already addressed under Article 28 (Section 0.2); technical architecture information already covered in Records of Processing Activities (ROPAs) and internal IT governance documentation (Section 1.3); and cybersecurity risk assessments already required under NIS2, the AI Act and DORA (Section 4). Controllers should not be required to reproduce this information within the DPIA.

Finally, the prescriptive nature of the template risks complicating compliance for organisations operating internationally. Many global controllers manage complex, multi-jurisdictional privacy requirements by developing standardised, internal DPIA frameworks designed to meet global needs. By introducing rigid structural mandates, the EDPB template makes it increasingly difficult for organisations to harmonise their global approach to DPIAs, ultimately increasing administrative friction without a corresponding uplift in data protection.

DOT Europe's Key Recommendations

Voluntariness: Maintain the optional character of the template to preserve organisational flexibility and avoid retroactive compliance burdens.
Proportionality: Clearly distinguish mandatory fields from optional ones, and indicate where a limited level of detail is appropriate.
No duplication: Remove or mark as optional requirements that duplicate existing obligations under Art. 28 GDPR, ROPAs, NIS2, DORA, and the AI Act.
Programme-level recognition: Explicitly accept programme-level documentation (project trackers, governance workflows) as a valid compliance mechanism.
AI Act alignment: Facilitate formal recognition of the DPIA as a sufficient basis for FRIA compliance where scope overlaps, avoiding parallel assessments.
Flexible format: Replace rigid table structures with free-text fields proportionate to the nature and risk level of the processing activity.

Confidentiality guidance: Provide clear guidance on the treatment of confidential DPIA content, particularly in the processor-to-controller context.

0. Overview of the processing

The DPIA technical sheet introduces a significant amount of additional documentation requirements that may not in all cases, add value while proving burdensome for organisations, hence be disproportionate particularly where mature compliance frameworks are already in place. In particular, requirements such as maintaining a detailed history of changes made to the information contained in the DPIA template, as well as documenting the specific roles, tasks, and responsibilities of all team members involved in the assessment process, risk creating unnecessary administrative overhead without necessarily improving data protection outcomes.

DPIAs should remain practical, risk-based, and outcome-oriented tools that support accountability and effective risk management, rather than becoming excessively procedural or documentation-heavy exercises. A large-scale AI system involving special category data and a straightforward employee directory should not demand the same depth of documentation. Many organisations already rely on established internal governance structures, project management tools, and audit processes that ensure appropriate accountability and traceability, in line with the GDPR's risk-based approach. Requiring companies to duplicate this information within the DPIA itself could lead to significant resource burdens, particularly for companies managing multiple or iterative processing operations across products, services, or jurisdictions. We, therefore, believe that the Template should explicitly recognise programme-level documentation as a valid and sufficient means of demonstrating compliance.

Section 0.2 – Sub-processors

The template should not require a detailed listing of sub-processors and contractual tasks that are already addressed through, and redundant with Article 28 GDPR. This creates duplication without added value.

Section 0.4 – Dates and Implementation Plans

Requirements for fixed "estimated launch dates" and "end dates", as well as detailed static implementation plans (Section 4.2.c), do not reflect the operational reality of modern digital services, where processing activities are subject to continuous iterative development. Furthermore, the structure of the template implies that a distinct DPIA is expected for every individual product 'launch'. We recall that the WP29 Guidance explicitly permits DPIAs to cover 'a set of similar processing operations'. Assessing risks at the level of similar processing operations, rather than demanding documentation for

every discrete launch, is a vital operational efficiency that should be preserved in the template. Consequently, implementation is most effectively managed through living operational systems that are continuously updated. The DPIA should document the what and why of risk mitigation; the when, who and how of implementation should remain in operational tooling appropriate to the organisation's processes.

Section 0.5 – Scope Documentation and Confidentiality

The template should not principally require the documentation of processing not covered in the DPIA and the reasons why it is not covered. Such a requirement risks creating an unnecessary inventory of features, configurations, integrations and deployment choices that are outside a particular use case, without added value and without basis in the GDPR.

The template should also not imply that publication or external sharing of the DPIA is expected. DPIAs may contain confidential information about controls, infrastructure, risk assumptions, mitigation strategies, contractual arrangements, system architecture and operational dependencies. The template and its Explainer should provide clear guidance on the treatment of confidential information, particularly in the context of processors providing information to controllers in support of the controller's as well as in joint-controllers scenarios. The guidance should explicitly reaffirm that controllers are not required to compromise trade secrets, intellectual property, confidential business information, or disclose systemic vulnerabilities in order to fulfil the extensive documentation requirements of the DPIA.

Section 0.6 – Societal Context

The inclusion of changes in 'societal context' as a reason to conduct a DPIA introduces an unfixed and highly subjective criterion. Without further parameters, this is likely to prove highly onerous and confusing, particularly for smaller organisations that lack the resources to continuously monitor abstract shifts in societal sentiment. We recommend explicitly anchoring this factor to the explanatory examples previously provided in the WP29 Guidance, such as instances where the effects of automated decisions become significantly more impactful or where new groups of data subjects become vulnerable to discrimination.

1. Systemic description of the processing

Section 1 splits the processing description into an unnecessarily granular set of sub-categories (personal data categories, purposes, operations, scope, context, functional description, data lifecycle, technical means, supporting assets), mirroring a RoPA structure rather than what Art. 35(7)(a) requires for a "systematic description of the envisaged processing operations and the purposes."

Section 1.1.c – Secondary and Compatible Uses

This sub-section asks controllers to provide information about secondary and compatible uses of the data involved in processing. But in many cases, secondary purposes of processing (and any compatibility assessment carried out with respect to them) may not be known at the time an initial DPIA is conducted. Less sophisticated controllers may struggle with this section if they misunderstand it as needing to be completed in every case and requiring them to anticipate all potential secondary uses before ever actually embarking on them. We recommend the EDPB to add "if known" to this sub-section of the template.

Section 1.2 – Data Flows Diagrams

The instruction that templates "should be supplemented with one or more diagrams representing data flows or a similar figure." should be clarified to specify that these diagrams should represent data flows at an entity level. Implying an obligation to construct highly detailed technical flow diagrams to the level of individual assets is extremely challenging, particularly for controllers using a network of processors whose technical information may fairly be outside the controller's knowledge. Without clarification, this requirement places a disproportionate burden on controllers.

Section 1.3 – Underlying Architecture

The requirement to describe the "underlying architecture" of the processing operation under point 1.3 may require organisations to provide a level of technical and operational detail that goes beyond the purpose and scope of a DPIA under Article 35 GDPR. In practice, this information is likely to overlap with existing Records of Processing Activities (ROPAs), security documentation, and internal IT governance processes, creating unnecessary duplication and additional administrative burden for organisations. Indeed, the level of granularity described in the DPIA template explainer, including detailed descriptions of hardware, infrastructure, network assets, software, and their grouping by logical module, technical layer, or function, appears overly prescriptive and risks going beyond what is necessary for a DPIA. Controllers, and in particular medium-sized organisations without dedicated privacy teams or specialized tooling, will struggle to produce this level of documentation for each processing activity requiring a DPIA.

Organisations should retain sufficient flexibility to determine the appropriate level of detail based on the nature, complexity, and risk profile of the processing activity with cross-references to specialist documentation where appropriate. We, therefore recommend that the Template should provide more flexibility both structurally , by marking sections as optional or conditional based on the type of processing, and in terms of format, by replacing rigid table structures with free-text fields that allow controllers to document their assessment in a manner proportionate to the processing at hand. A DPIA is a substantive analytical exercise, not a form-filling exercise.

2. Analysis of the processing

Section 2.2.2 – Data Quality Metrics

The data quality section (Section 2.2.2), which requires organisations to provide data quality metrics, requirements, or thresholds, appears to go beyond the requirements set out under Article 35 GDPR.

Requiring specific metrics for processing activities may create unnecessary complexity and prescriptive compliance obligations, particularly given the wide variety of processing operations and business models covered by the GDPR. Instead, this section should focus more broadly on how organisations ensure and maintain data accuracy, which is already addressed under Section 2.3 in relation to the accuracy principle. This would better align the template with the GDPR's risk-based and proportionate approach.

Section 2.2.3 – Implementation Status Labelling

The mandatory implementation status labelling (Planned / Partially Implemented / Implemented) across Sections 2.3.a–e assesses compliance maturity, whether a measure has been deployed, rather than whether the processing poses a risk to data subjects. This is a compliance management function that falls outside the scope of Art. 35(7). It should either be removed or made optional.

4. Risk Assessment and Management

Section 4, which focuses on malfunctions and deviations from design and default, appears to go beyond the scope of a traditional DPIA under the GDPR and moves closer to a broader cybersecurity or AI risk assessment exercise.

In particular, the extensive list of risk sources, including software bugs, misconfigurations, wrong access rights, operational errors, lack of maintenance, insider abuse, and external attacks, risks creating a highly burdensome and overly expansive assessment obligation for organisations. Requiring companies to systematically assess such a broad range of technical and operational risks within the DPIA framework may duplicate existing security, cybersecurity, and enterprise risk management processes under other framework such as NIS2, AI Act and DORA, while extending beyond the legal scope and purpose of Article 35 GDPR.

Interplay with the AI Act

The Template presents an overlap between Article 35 GDPR and the Fundamental Rights Impact Assessment (FRIA) required under Art. 27(1) of the AI Act for deployers of high-risk AI systems.

The FRIA and the DPIA share substantial common ground: both assess risks to fundamental rights, both require a description of the processing and its purposes, and

both mandate the identification of mitigation measures. For controllers deploying high-risk AI systems, these assessments will frequently cover the same processing activity, the same data subjects, and many of the same risks.

A template genuinely aimed at enhancing consistency across the EU, the EDPB's stated objective would acknowledge this overlap and facilitate alignment between the two assessments. In practice, this means the template should be recognised by the EU AI Office as a sufficient basis for meeting FRIA obligations where scope overlaps; it does not mean incorporating AI Act-specific requirements into the DPIA template itself.

At a time when the European Commission's stated objective is regulatory simplification, and when controllers are actively preparing to comply with the AI Act's obligations, this is a missed harmonisation opportunity that will result in parallel, redundant documentation without uplift in data protection outcomes.

Section 4.1a – Risk Sources

The Template tasks controllers with identifying "[r]isk sources (exposures and errors, vulnerabilities etc.)." Controllers, especially smaller controllers, often lack the deep cybersecurity expertise required to document granular threat vectors. We recommend that this be simplified (or up-levelled) to better accommodate less sophisticated controllers while still enabling satisfactory assessments.

5. Data Protection by Design and by Default

The template's expectation of a dedicated, standalone section on Data Protection by Design and by Default (DPbDD) (Art. 25 GDPR) may inadvertently encourage a box-ticking approach, where measures are listed in the abstract rather than demonstrated in the context of the specific risks they address. DPbDD is most effectively evidenced when integrated within the risk assessment itself, showing how design decisions and embedded safeguards directly reduce identified risks to data subjects. The template should allow organisations to demonstrate DPbDD contextually, rather than requiring a separate section that risks duplicating information already present in the risk mitigation analysis.

Conclusion

DOT Europe supports the EDPB's objective of improving consistency in how DPIAs are conducted across the EU. A well-designed common template can serve as a genuine tool for data subject protection, providing controllers with a clear framework for risk identification and mitigation. We recognise that effective DPIAs benefit data subjects directly, and our recommendations are made in that spirit.

At the same time, the current draft risks undermining those objectives by shifting the DPIA process from a substantive risk-based exercise to a prescriptive documentation exercise. The concerns identified in this response, disproportionate administrative requirements,

duplication of existing obligations, absence of mandatory/optional distinctions, and failure to align with the AI Act's FRIA, are not merely operational inconveniences. They risk producing DPIAs that are formally compliant but substantively hollow, which serves neither data subjects nor regulators.

DOT Europe therefore calls on the EDPB to revise the template in line with the four key principles reflected throughout this response:

Summary of Key Asks
Voluntariness: Maintain the optional character of the template; avoid prescriptive minimum requirements that extend beyond Art. 35(7) GDPR.
Proportionality: Mark sections as optional or conditional based on the type, complexity, and risk level of the processing activity.
Coherence: Remove duplication with Art. 28, ROPAs, NIS2, DORA, and the AI Act; recognise programme-level governance as sufficient.
Alignment: Facilitate formal recognition of the DPIA as a sufficient basis for AI Act FRIA compliance where scope overlaps.

DOT Europe would welcome the opportunity to discuss these recommendations further with the EDPB and stands ready to contribute to a revised template that genuinely advances data protection outcomes across the EU.