

d.pia.lab contribution to the EDPB Public Consultation on a DPIA Template and Explainer

Draft DPIA Template and Explainer (Version 1.0, adopted 10 March 2026)

Maciej Otmianowski,^α Alessandra Calvi,^{αβ} Simone Casiraghi,^α Cesar Augusto Fontanillo Lopez,^χ Pia Groenewolt,^α Federica Paolucci,^δ Natalia Ribeiro Lopes de Paulo,^α Ine Van Zeeland,^α Niels Van Dijk^α

Executive summary

On 14 April 2026, the European Data Protection Board (EDPB) opened a public consultation regarding the template for data protection impact assessment (DPIA) and its respective explainer. As stated in the accompanying information concerning the public consultation,¹ at the end of the consultation, data protection authorities (DPAs) will “begin the necessary steps to adopt this template as their unique template or as a ‘meta-template’, with which national-specific templates will be compatible”.

This contribution, which offers the analysis of the draft EDPB DPIA Template and the accompanying Explainer, conducted by the d.pia.lab team and associates, pursues highlighting opportunities to enhance the methodological approach for the template. The most important recommendations are following:

1. The consultation should be situated within the context of the Digital Omnibus discussions on the role of the EDPB DPIA template as a common tool.
2. To assist controllers in the compliance with their legal requirements, and truly serve simplification and clarification purposes, greater coordination with other GDPR obligations (e.g., registry of processing activities, legitimate interest assessment) as well as relevant rules of the body of EU digital law (e.g., publicity requirements and coordination with the Fundamental Rights Impact Assessment under the EU AI Act) needs to be envisaged.
3. The interaction between proportionality and risk assessment should be clarified, as well as the structure and scope of the assessments themselves.
4. Key concepts should be clearly defined in a dedicated glossary.

^α Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab), Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB)

^β CY Cergy Paris Université, ENSEA, CNRS | ETIS UMR 8051

^χ Centre for IT & IP Law (CiTiP), KU Leuven

^δ Baffi Centre, Bocconi University

¹ https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en

5. Baseline criteria for risk acceptance, severity, and likelihood, as well as for the “least intrusive” test, should be clearly defined.
6. Data subject consultation should be integrated throughout the impact assessment process (e.g., risk identification, risk treatment, and fair balancing). In addition, the wording “when relevant” in Article 35(9) should be operationalised and clarified.
7. Publication of DPIA results, although not required, should be encouraged where appropriate. We recommend creating a public database of accessible DPIA results, preferably in a machine-readable format and supported by open-source software.
8. Clear guidance should be provided on preparing DPIA summaries for public access, including alignment with AI Act requirements.
9. The template may also be conceived as an accountability tool enabling controllers to demonstrate why a DPIA was not required.
10. The DPIA structure should enable the assessment when concerns the deployment of a technology or system (such as an AI system or enterprise tool) that is then used across multiple distinct processing activities.
11. The EDPB may consider distinguishing between what is mandated by law and what they recommend based on their previous opinions that are referred to in the explainer but not sufficiently elaborated upon.

Table of content

<i>Executive summary</i>	- 1 -
<i>Introduction</i>	- 3 -
<i>Comments on the consultation context</i>	- 4 -
<i>Comments on the Structure of the Template and Explainer</i>	- 5 -
<i>Comments on the Sections of the Template and Explainer</i>	- 6 -
<i>Final remarks</i>	- 14 -
<i>Acknowledgments</i>	- 14 -

Introduction

The Brussels Laboratory for Data Protection & Privacy Impact Assessments, or d.pia.lab, connects fundamental, methodological and applied research and delivers policy advice related to impact assessments in the areas of innovation and digital technology development. Whilst legal aspects of privacy and personal data protection constitute its core focus, the d.pia.lab includes other disciplines, including ethics, philosophy, surveillance studies and science, technology & society (STS) studies. Established in November 2015, the Laboratory constitutes a part of and builds upon the experience of the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB), Belgium.

As researchers affiliated with the d.pia.lab, a network of legal and philosophical scholars focused on data protection, AI regulation, and risk and impact assessments, we welcome the opportunity to contribute to the European Data Protection Board public consultation regarding the Template for data protection impact assessment (DPIA) and its Explainer. DPIAs represent a methodical and considered approach to ensuring that risks are properly identified, assessed, and mitigated in order to protect data subjects. The d.pia.lab therefore strongly supports the development of a common DPIA methodology, in which the development process is transparent, participatory, and open to contestation. The draft Template and Explainer provide a valuable and comprehensive effort to support assessors in conducting Data Protection Impact Assessments under Article 35 GDPR. We welcome some features of the template, such as the focus on data subjects' perspective; the separation of the explainer from the actual template; the possibility to integrate and cross-reference parts thereof; the structured approach; the integration of examples and the attempt to guide risk analysis in a practical manner. The document has the potential to contribute significantly to more consistent and structured DPIA practices across organisations and contexts. However, we have identified several points for improvement, which are discussed in this contribution. We do not want to diminish the effort of the EDPB in that respect. The methodology needs to find a compromise across multiple DPAs equipped with different resources and operating in different legal traditions. It needs to produce an explainer and a template suited to be used by controllers of multiple sizes (from SMEs to big techs), with different expertise and resources. These documents need to be, at the same time, user-friendly and easy to complete but also capable of triggering the critical thinking of their users, to avoid a DPIA turning into a mere check-boxing exercise, instead of a tool to actually inform decision-making, enhance risk-based knowledge, and mitigate risks for all types of data subjects.

Our contribution is structured as follows. First, it provides general comments on the context of the consultation and the role of the DPIA methodology provided by the EDPB. Next, it presents comments on the structure of the DPIA Template and the Explainer. The rest of the comments and recommendations are then organised according to the order of sections in the Template and Explainer. The comments below aim to further strengthen the Template's conceptual coherence, methodological clarity, and practical usability, ensuring it supports controllers to respect fundamental rights of data subjects, rather than merely document compliance in a fragmented, checkbox-driven manner.

Comments on the consultation context

The ongoing discussions on GDPR practice and its future evolution remain central to this consultation. We therefore situate our comments within the broader context of the European Commission's Digital Omnibus proposal, which aims, among other objectives, to “simplify, clarify and improve the European Union (EU) acquis” on digital regulation. The Digital Omnibus proposal of November 2025 advanced the idea to amend Article 35 General Data Protection Regulation (GDPR) to create more uniformity and certainty as regards the notion of high-risk by introducing EU-level lists of processing operations (not) requiring a DPIA. Furthermore, the EDPB shall prepare a “proposal for a common template and common methodology”, in line with its July 2025 Helsinki Statement,² for conducting DPIAs and transmit it to the European Commission, which will then review and adopt it as a delegated act. While at the time of writing, an agreement on the Digital Omnibus has yet to be reached, we will provide feedback on the Template and Explainer, considering such goals of simplification, clarity, and improvement of the EU acquis in mind. We assume that this template will eventually become the main term of reference for data controllers carrying out DPIAs under EU law. Once published and adopted in practice, it may shape compliance behaviour across EU Member States, but potentially also beyond the EU, especially where organisations align their data protection practices with EU standards. For that reason, the template warrants close scrutiny, particularly in light of the regulatory effects it may produce as a practical benchmark for DPIA compliance.

Against this backdrop, we were surprised to note that the EDPB did not frame such a consultation in the light of the Digital Omnibus discussion, especially concerning the role that the DPIA will serve in connection with other impact assessments. In turn, the EDPB expressly stated in the first page of the explainer that the template has a significantly more “modest” ambition to “record the most important results, a minimum amount of information that should always be documented, in the format adopted by the EDPB and easily accepted” by all DPAs. Furthermore, the EDPB did not take a stance on DPIA methodology, stating that “Controllers can conduct their risk analysis and management processes as they prefer, using the DPIA methodology of their choice (see Annex A)”.

While this could be motivated by pragmatism to allow for different contexts, it could also be partly motivated by the lack of certainty as to the outcomes of the Digital Omnibus procedure, and the difficulties of obtaining a compromise among the various DPAs on controversial methodological aspects. However, if the EDPB template and explainer were elaborated to provide more clarity and simplification, we do not think that, in their current form, they fully achieve such goals.

We are not convinced that turning this template into a “meta-template” containing only the minimum elements of a DPIA would improve clarity or simplify it. Instead, it risks creating an

² European Data Protection Board (EDPB), *The Helsinki Statement on enhanced clarity, support and engagement: A fundamental rights approach to innovation and competitiveness*, adopted on 2 July 2025, available at: https://www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf

unnecessary layer of duplication whereby controllers will continue to rely on their own templates and methodologies while, at the same time, striving to comply with the meta-template. It is also possible that some controllers relying on more developed methodologies change their approach to comply with such minimal requirements, which in the worst case could ultimately drive a “race to the bottom” in DPIA practices.

Comments on the Structure of the Template and Explainer

0 (General structure) — Template and explainer

Comments: The Template appears to assume that the DPIA concerns a single, bounded *processing activity* as the object of assessment (for example, as implied by Section 0.3). This assumption does not apply to situations in which a DPIA concerns the deployment of a technology or system (such as an AI system or enterprise tool) that is then used across multiple distinct processing activities. This limitation matters in practice because controllers frequently perform DPIAs for tools and processes that operate in heterogeneous contexts (e.g., when the single AI system is being implemented in many different processing activities). In such cases, the risk profile can vary substantially depending on the purpose of use, the categories of data subjects affected (e.g., employees compared with minors or other vulnerable individuals), and the operational environment.

In its current form, the Template does not adequately support differentiation between these contexts, nor does it facilitate repeating risk, necessity, and proportionality analysis per context. As a result, there is a material risk that controllers will describe the tool generically while under-analysing the contextual variation that determines the risk level and the necessity and proportionality balance.

The Template and Explainer do not explicitly recognise links with other existing GDPR requirements. Assessments should build on existing knowledge of data processing activities, such as the Register of Processing Activities (Art. 30 GDPR) and security or risk assessments (Art. 32 GDPR). This may result in an excessive burden on data controllers and inconsistencies in data protection systems within organisations.

Recommendations:

- The Template should explicitly allow for a multi-processing DPIA structure. Where a system supports multiple processing activities, the Template should require context-specific repetition of the core analytical parts (in particular, Sections 1–4) so that the assessment captures differences in context, purpose, and data subject categories. To enable this, Section 0 should include a short introductory statement clarifying whether the DPIA concerns a single processing activity or a system affecting multiple processing activities, and how those activities are delineated for assessment.
- Regarding publishing the assessment, the current template presents a binary choice: publish the DPIA in its entirety or not at all. There should be more nuanced options presented: assessments can be published in part, for instance without (security-)

sensitive information. Reference with transparency provisions enshrined in other legal instruments ought to be envisaged (e.g., Annex VIII Section C (5) AIA).

- The Template and Explainer should explicitly recognise and integrate links with other GDPR requirements, ensuring that assessments build on existing knowledge, including the data protection by design (Art. 25 GDPR) Register of Processing Activities (Art. 30 GDPR) and risk assessment (Art. 32 GDPR).

Comments on the Sections of the Template and Explainer

0.1–0.2 — Controller(s) / Processor(s) — Template

Comment. Sections 0.1 and 0.2 are under-specified and rely on open-ended descriptors, such as “information about the DPO” and “definition of obligations and tasks.” This drafting approach is likely to lead to inconsistent reporting, reduce comparability between DPIAs, and weaken operational clarity regarding risk governance responsibilities. A notable gap is that the Template does not explicitly identify who is responsible for risk acceptance decisions (a question that becomes central later, particularly in Section 4). In addition, joint controllership relationships are not represented in a sufficiently structured manner to support consistent allocation of responsibilities.

Recommendation:

- The Template should introduce mandatory structured fields capturing, at minimum, identity, function, contact details, and explicit responsibility for risk decisions. It should also include dedicated structures for joint controllers, requiring explicit allocation of responsibilities, including responsibility for residual risk acceptance and decision-making roles relevant to DPIA outcomes.

0.5 DPIA technical sheet — Template

Comment. Section 0.5 aggregates conceptually distinct elements in a single place: DPIA trigger criteria (threshold analysis), versioning/logging, scope definition, team composition, and publication choices. This aggregation creates conceptual ambiguity and increases the risk that controllers misunderstand DPIA triggers. It may also generate legal uncertainty when a checklist-based threshold evaluation is completed incorrectly or prematurely, especially when the checklist is treated as a definitive legal conclusion rather than a reasoned assessment. Furthermore, it undermines the accountability of data controllers’ obligations, as it is equally important to document cases where specific processing activities do not require a DPIA. Additionally, the concept of “scope” (what is included/excluded) overlaps with Section 1.1.d (nature/scope/context), potentially leading to duplication or inconsistency. Team information is also unclear as to whether it should reflect all contributors across the DPIA lifecycle. And it lacks the requirement to provide information about the expertise brought to the assessment.

Recommendation:

- Threshold analysis (as a legal obligation under Article 35) should be separated from documentation management (versioning and publication). The Template should require explicit specification of the expertise of all involved participants (internal and external). It should clarify whether threshold determination is intended as a final conclusion or a provisional judgement that may change as information becomes available.
- The Template should also be conceived as an accountability tool that controllers may use to demonstrate why a DPIA was *not* required in the case of specific personal data processing.³
- The Template should also clarify how Article 32 residual risk considerations interact with DPIA necessity—specifically, whether persistently high residual risk to a right to rights and freedoms of natural person under data security evaluation is treated as a trigger or indicator that a DPIA is required or must be revisited.

1. SYSTEMATIC DESCRIPTION OF THE PROCESSING

1.1.a Processed personal data — Template

Comment. The table design appears to follow a data inventory logic rather than a risk-oriented DPIA methodology. By prioritising categories of personal data without systematically linking them to data subject roles and processing contexts, it may obscure how specific data uses generate risks, including indirect discrimination risks that do not necessarily involve Article 9 special categories.

Recommendation:

- The table should be restructured around (1) data type, (2) data subject category/role, and (3) special category status. The Template and/or Explainer should explicitly acknowledge that non-Article 9 data (e.g., age or gender) can nevertheless generate significant risk in certain processing contexts, including discrimination, exclusion or unfair treatment, especially in automated decision-making.

1.1.c Secondary uses — Explainer (para. 14)

Comment. The compatibility analysis described in paragraph 14 does not sufficiently reflect contemporary processing realities. In particular, it does not explicitly address the use of data for AI model training, data sharing under EU data governance regimes, or disclosure obligations that may compel re-use or access.

³ See. Kloza, D., Calvi, A., Casiraghi, S., Vazquez Maymir, S., Ioannidis, N., Tanas, A., & Van Dijk, N. (2020). Data protection impact assessment in the European Union: developing a template for a report from the assessment process. d.pia.lab Policy Brief , 2020 (1), 1-52. <https://doi.org/10.31228/osf.io/7qrfp>, <https://doi.org/10.5281/zenodo.4501295>

Recommendation:

- The Explainer should explicitly include AI training uses, data sharing frameworks, and legal disclosure obligations within the compatibility assessment prompt, so that controllers systematically evaluate these pathways. It includes engagement with the requirements of the Data Governance Act and Data Act.

1.2 Functional description — Template & Explainer (para. 19)

Comment. The term “use” is overly generic and does not correspond to GDPR definition, risking incomplete description of processing operations.

Recommendation:

- The Template and Explainer should require alignment with the Article 4(2) GDPR list of processing operations. The Explainer should also clarify obligations regarding deletion oversight, including how responsibility is shared between controller and processor for verifying deletion and erasure.

2. ANALYSIS OF THE PROCESSING

2.1 Lawfulness — Explainer (paras. 22–24)

Comment. While the Explainer appropriately addresses the identification of the legal basis, it does not explicitly distinguish this step from the assessment of risks in the DPIA. Compliance with Articles 6 and 9 GDPR does not, in itself, demonstrate that the risks to individuals are acceptable under Article 35, as lawful processing may still entail high risks requiring mitigation or redesign.

Recommendation:

- The Explainer should explicitly clarify that lawful processing does not necessarily mean the risks to individuals are acceptable. It should also make clear that the analysis of lawfulness is a distinct step and does not replace the necessity and proportionality assessment or the identification and mitigation of risks.

2.3 Compliance measures — Template & Explainer

Comment. The selection of measures lacks clear criteria and omits relevant GDPR obligations, particularly those relating to children’s consent (Article 8) and breach procedures (Articles 33–34). This omission is significant because DPIAs are intended to connect compliance measures with the management of risks to rights and freedoms.

Recommendation:

- The Template and Explainer should explicitly include these obligations and clarify the selection logic for “other GDPR requirements,” ensuring that controllers understand why particular measures appear and how to document them consistently.

Pleinlaan 2 ▾ 1050 Brussel

3. NECESSITY AND PROPORTIONALITY

General structural issue — Sections 3 vs 4

Comment. The relationship between Section 3 (necessity and proportionality assessment) and Section 4 (risk assessment) in the consulted documents remains unclear. Three issues follow. First, there is no clear analytical sequencing: risks in Section 4 may be assessed without being properly integrated into necessity and proportionality analysis. Second, the structure implies that risk analysis proceeds independently of legality constraints; however, if a processing is not necessary or proportionate, risk mitigation may become secondary because the processing should be redesigned or not proceed. On the other hand, to ensure a fair balance of rights and interests in the proportionality assessment, the risks to rights and freedoms should be identified and assessed (e.g., AEPD DPIA methodology).

Recommendation:

- The Template and Explainer should clarify the relationship between the Section 3 (necessity and proportionality assessment) and Section 4 (risk assessment). First, whether necessity and proportionality function as legal prerequisites or as part of a broader balancing exercise. Second, they should also clarify the relationship between Explainer paragraphs 32-34 (Section 3) and paragraphs 35-43 (Section 4), including how outputs from one part are meant to inform the other.

Methodological issue relevant for 3 & 4 sections (proportionality & risk assessments)

Comment. We welcome the distinction between risks (“threats”) posed by the processing “as it has been designed” (template pt. 3.1) and risks (“threats”) arising from malfunctions, deviations, or data security issues (template pt. 4.1(a)). However, the template does not explain why one type of risk is addressed in the necessity and proportionality assessment, while the other is placed in the risk assessment section. In our view, both types of risks should fall within the scope of risk assessment and management.

Second, the distinction between “risk” and “threat” is blurred. Third, the assessment is not grounded in a structured causal model. There is a need to identify explicitly which rights are affected, to articulate impact scenarios as causal chains, and to include the perspectives and interests of data subjects in the analysis.

Recommendation:

- Both types of risk should be addressed in the risk assessment and management section. The template should clarify and explain the causal chains for each type of risk, including their direct link to rights and freedoms (processing → event/condition → consequence → interference with a specific right). The clear definitions and consistent terminology should be used. The results of the risk assessment and management should then be taken into account in the necessity and proportionality assessment. Additionally, disproportionate processing activities should be considered unacceptable.

3.1 Impacts — Explainer (para. 32)

Comment. Paragraph 32, on risk scenario, lacks conceptual clarity. What rights should be considered in the assessment (primary, secondary EU law, and/or national law). In our view, this should at least include the rights set out in the EU Charter. However, it remains unclear whether rights established in secondary EU law and giving further substance to the rights enshrined in the Charter—for example, the right of withdrawal from a contract and others under the Consumer Protection Directive (Art. 9, 2011/83/EU)—should also be included. If that is the case, it is then unclear whether the assessment should also cover rights provided under the national laws of the Member State where the data subject resides, including constitutional rights or other statutory rights. Clear guidance from the EDPB on the scope of relevant rights would therefore be very helpful.

Recommendation:

- The Explainer should provide clarification on what rights and freedoms should be considered in the assessment and how they should be identified in the data controller's context.

3.2 Necessity — Explainer (para. 33)

Comment. Three issues arise. First, the term “effective” is conceptually inappropriate for necessity analysis; it risks shifting attention toward operational efficiency rather than legal suitability. It should assess whether a measure has the potential to achieve its legitimate purpose, but it should not test which measure is the most effective. The assessment should remain neutral, in order to avoid balancing effectiveness against the interference with rights and freedoms. The comparison should focus on whether each measure is capable of achieving the purpose, and then determine which option is the least intrusive (in the next step). Second, the Explainer does not indicate how the “least intrusive test” is to be performed and does not require mandatory comparison with alternatives. Third, there is no requirement for controllers to define evaluation criteria, which may allow necessity to be asserted without transparent or verifiable standards.

Recommendation.

- Paragraph 33 should replace “effective” with “suitable.” It should further require identification of alternatives and justification for rejecting less intrusive measures. Finally, it should also require controllers to define their necessity criteria and explain how reassessment will occur, so the DPIA can support ongoing accountability rather than a one-off justification.

3.3 Proportionality — Explainer (para. 34)

Comment. Paragraph 34 raises three conceptual concerns. First, its wording can be read as encouraging a cost-benefit approach to proportionality. Second, the reference to “collectively” is unclear and not operationalised, leaving unclear what it refers to. Third, the proportionality assessment is insufficiently linked to the impacts identified later in the DPIA and to the results of the risk assessment (especially with respect to severity).

Recommendation.

- Paragraph 34 should clarify that proportionality is not a cost-benefit analysis but a legal balancing of rights and interests, where the protection of rights retains primacy. It should define “collectively” or remove the term if it cannot be operationalised. Finally, it should require explicit cross-references to Section 3.1 (identified impacts) and Section 4 (severity of risks) so that proportionality recognises the identified risk landscape.

4. RISK ASSESSMENT AND MANAGEMENT

4.1.b — Risk assessment method - Explainer (para. 36)

Comment. Minimum standards do not accompany methodological flexibility, ensuring consistency. In the absence of minimum methodological standards, data controllers may develop divergent assessment methods, which may lead to inconsistent assessments and undermine the comparability and reliability of DPIA outcomes and fundamental rights protection. While such standards inevitably constrain methodological flexibility, they still leave sufficient room for manoeuvre to adapt assessments to specific contexts. In particular, the Explainer sets no baseline expectations for likelihood, severity, or risk acceptance. This may lead to divergent or inconsistent assessments and undermine the comparability and reliability of DPIA outcomes.

Recommendation:

- The Explainer should complement methodological flexibility with some minimum standards. It should require explicit definition of scales, documentation of assumptions, and identification of acceptable risk thresholds (including what constitutes “non-acceptable” risk and how that threshold is determined).

4.1.c — Inherent risk assessment - Explainer (paras. 37–40)

Comment. Several conceptual ambiguities remain in the description of inherent risk assessment. The definition of risk is incomplete, as it lacks a clear causal chain outlining the relationships between causes and effects in the risk scenario. The relationship between likelihood and the individual elements of the causal chain is unclear. It is not evident what exactly the likelihood is supposed to assess; severity is not sufficiently tied to fundamental rights; and the link to processing characteristics described in Section 1 is weak.

Recommendation

- The Explainer should clarify how the concepts of inherent and residual risks are understood in the method (perhaps in a glossary). We emphasise the importance of exploring how the risk scenario links processing to potential interferences with rights. The understanding of the likelihood should be specified, whether it is the possibility of an event and/or the potentiality of rights infringement (as a result of the event). In particular, it should be clarified whether likelihood refers to the occurrence of an event

(e.g., loss of confidentiality), to the likelihood of an infringement of a fundamental right resulting from such an event, or to the likelihood of an infringement arising directly from the processing activity itself—or possibly to all of these. The logic(s) must be chosen and used consistently. Severity should be assessed to determine whether the interference with a fundamental right constitutes an infringement. Finally, the Template should require explicit linkage between each identified risk and the relevant processing characteristics (including purpose, context, scope and means of processing).

4.2 — Action Plan - Explainer (paras. 41–43)

Comment. Three points of improvement can be flagged. First, while paragraph 41 defines “additional measures” as those not initially planned, it remains unclear what should be considered “initial”. In particular, it remains unclear whether this refers to the situation prior to the DPIA, prior to the risk assessment or prior to the mitigation phase. This ambiguity affects the distinction between inherent and residual risk and may lead to inconsistent interpretation. Second, while briefly mentioned in paragraph 39, it is not specified how risk acceptance decisions are governed (i.e. what acceptability means, for whom, how it should be determined, and what the thresholds are). Risk acceptance governance is not specified. Third, the mitigation process is insufficiently operationalised.

Recommendation:

- The Explainer should require that measures be explicitly linked to risks, identify responsible actors, resources, and timelines, and document who accepts residual risk and on what criteria, including the DPO’s role in that decision, where relevant. The mitigation must include responsibility, resources, deadlines and evaluation criteria—not just a list of safeguards. Guidance should be provided on how to determine acceptance criteria.

5. INVOLVEMENT OF DATA PROTECTION OFFICER AND DATA SUBJECTS

Comment. The Template marginalises DPO input and involvement of data subjects and their representatives. While this aspect is addressed, placing involvement at the end of the document/process may give the impression that participation is an afterthought. In contrast, it should be encouraged throughout the assessment. This may weaken the overall robustness of the assessment, particularly the proportionality analysis, especially where balancing interests requires understanding affected persons’ perspectives.

Recommendation:

- The Template should require documentation of DPO advice, how it was implemented, and how disagreements were resolved on each stage of the assessment process. The Explainer should also encourage and provide practical mechanisms for the involvement of data subjects and their representatives. It should also explain how the preliminary identification of relevant data subjects or their representatives was made and explain their participation in the DPIA process. At these stages, through which means, based on what information, what they could do, etc. We particularly encourage

the Board to provide clarification on when the data subject's involvement in the assessment is "appropriate" according to Art. 35(9) GDPR.

6. CONCLUSION & DECISION

Comment. Technical inconsistencies, as well as the absence of a structured follow-up logic (i.e., the mechanisms that ensure the DPIA is revisited, updated, and remains valid over time) reduce the usability of the template. The lack of the public accessibility can undermine the DPIA's function as a living accountability instrument.

The issue of transparency is only vaguely addressed in the Template and Explainer. They do not provide any guidance on voluntary or mandatory transparency of assessments (e.g. in the context of the AI Act). This affects data controllers who are willing to share their assessments but do not know how to do so safely (e.g. while protecting trade secrets and intellectual property rights). It also limits the potential for engagement by the concerned public and public authorities with these assessments.

Recommendation:

- The Template should correct internal references, require review cycles, and update triggers so that DPIAs remain current as processing changes. Moreover, the template should provide guidance on how to summarise each stage of the assessment and its results for publication in the EU database required for high-risk AI systems under the AI Act (Art. 49(3), Annex VIII, Section C, point 5).
- The EDPB could encourage controllers to publish DPIAs and provide guidance on handling confidential, trade secret, and security-sensitive information. This could include publishing full DPIAs, anonymised versions, specific sections (e.g., risk assessments), or summaries highlighting identified risks, likelihood and severity, and adopted safeguards. Ideally, such disclosures should be in a machine-readable format to enhance transparency, comparability, and public scrutiny. In the longer term, the EDPB could consider establishing a public database of DPIAs or their extracts. This could be complemented by open-source software (similar to tools developed by CNIL or AEPD) to help controllers generate standardised, anonymised, and machine-readable outputs for implementation in compliance solutions. However, this should follow once the methodology has stabilised. Such measures would enable benchmarking, support empirical research on risks to rights and freedoms, and strengthen the traceability of data protection compliance practices, thereby advancing data protection enforcement and compliance more broadly.

Final remarks

The Template provides a comprehensive structure, but without clearer conceptual foundations, clearer analytical sequencing, and more explicit methodological requirements, it risks encouraging formalised completion of DPIAs without ensuring substantive assessment of risks to rights and freedoms, contrary to the purpose of Article 35 GDPR. Finally, efforts should focus on the interaction between the DPIA and the Fundamental Rights Impact Assessment (Art. 27(4) AI Act), in order to ensure compatibility and create synergies between the two assessments in the context of processing activities involving high-risk AI systems.

Although the GDPR was adopted more than ten years ago, many basic questions related to DPIAs remain unresolved. What is the exact scope of risks to rights and freedoms in a DPIA? How should the necessity and proportionality assessment be conducted? Is such test the same one that is performed in adjudication? How does this test interact with the safeguards already provided by data protection principles, such as lawfulness, fairness, data minimisation, and purpose limitation? How does it interact with the risk assessment? What types of risk scenario logic should the assessment include? Does the EDPB align with or endorse any specific methodologies? We remain open to further discussion on the topic of impact assessments.

Acknowledgments

This contribution is supported by project funding provided by the Research Foundation – Flanders [FWO reference no. G000724N] and National Science Centre [NCN reference no. 2022/47/I/HS5/02457] under the Weave initiative.