TILBURG INSTITUTE FOR LAW, TECHNOLOGY, AND SOCIETY
TILBURG UNIVERSITY

Tilburg Institute for Law, Technology, and Society's contribution to the public consultation on the European Data Protection Board DPIA Template

A. Tilburg Institute for Law, Technology, and Society (TILT) is one of the leading research groups in Europe at the intersection of law, technology, and society. Our research efforts are aimed at, among others, understanding the interaction of technology and social and normative practices in order to clarify how regulatory challenges of socio-technical change can be addressed.
B. TILT welcomes the European Data Protection Board's initiative to develop a common template for Data Protection Impact Assessments under Article 35 GDPR. The availability of a detailed template has the potential to promote greater consistency in the preparation of DPIAs across organisations and sectors, while supporting controllers in conducting more comprehensive and accountable assessments.
C. We consider this initiative particularly timely in light of the increasing complexity of personal data processing operations and the growing interaction between the GDPR and other areas of EU digital regulation. A harmonised approach to DPIAs can facilitate compliance efforts and improve the quality of risk assessments. Ultimately, this can help strengthen the protection of data subjects' rights and freedoms.
D. At the same time, we believe that certain aspects of the proposed template would benefit from further clarification and refinement. In particular, additional guidance could help reduce interpretative divergences, improve consistency among organisations conducting DPIAs, and better reflect existing GDPR requirements and relevant EDPB guidance.
E. We therefore welcome the opportunity to contribute to this public consultation and respectfully submit the following observations and recommendations.
F. The comments below first address several general aspects of the template and then provide more detailed observations concerning specific sections of the proposed DPIA framework.

A. General Comments

1. Descriptors and examples

The proposed template provides a comprehensive blueprint for conducting DPIAs. However, in several sections the descriptors remain relatively high-level and may still lead to divergent interpretations among organisations regarding the information expected and the level of detail required. We therefore recommend providing more detailed instructions for completing the various sections of the template and where possible, replace open-ended references such as "etc." or broad illustrative lists with more exhaustive indications of the information expected. Overall, more detailed guidance would promote greater consistency across DPIAs and improve the comparability

of assessments conducted by different organisations. Where appropriate, the template could also provide brief examples illustrating the type of information expected in particular fields.
We further recommend providing short explanations of terms that do not originate directly from the GDPR and may be interpreted inconsistently, such as "supporting assets".

2. Overlapping obligations between GDPR and other relevant EU digital regulations

EU digital law and data governance require organisations to complete multiple templates and periodically review them. The proposed template is GDPR-centric, but organisations increasingly operate under overlapping obligations.

- What shall be noted is that personal data protection and accountability emerge not just from a structured and reflected DPIA, but also from good strategies regarding security incidents and recovery strategies. These contexts involve dynamic, time-sensitive decision-making and legal interoperability challenges between GDPR and EU cybersecurity law. The template could include dedicated fields addressing temporary emergency processing, intersecting regulatory obligations, proportionality under operational urgency, and ex post accountability review.
- The DPIA template could prompt controllers to identify parallel legal obligations affecting necessity/proportionality analysis**.** We therefore suggest adding a section dedicated to relevant intersecting legal and regulatory obligations affecting necessity/proportionality analysis. This will allow entities to adequately map and better capture tensions such as GDPR minimisation vs logging requirements, purpose limitation vs incident intelligence reuse, storage limitation vs forensic preservation duties. For example, this would help ensure adequate mapping and better capture tensions such as GDPR data minimisation versus cybersecurity logging obligations under NIS2 or internal incident response requirements.
- Controllers may face difficulties when conducting DPIAs in areas characterised by legal uncertainty or evolving regulatory requirements. We recommend that the DPIA template allow controllers to document areas of legal uncertainty, including any interpretative ambiguities and consultation or escalation steps undertaken.
- We also recommend that the template allows controllers to explain how necessity and proportionality assessments may be affected by situations involving operational urgency or significant uncertainty.

3. The relationship between DPIAs and other AI-related compliance obligations

Where processing involves AI systems, particularly systems subject to obligations under the AI Act, the template could provide optional guidance on documenting relevant technical characteristics, human oversight measures, training data considerations, and interactions with AI Act compliance.

4. DPIA as a living document

Data risks frequently evolve over time. This may be linked to new processing activities, but also to updates in the processing already implied.
Therefore, we recommend that the template introduce a section regarding when the DPIA should be reviewed, what events trigger reassessment, whether periodic review intervals are defined and who is responsible for re-opening it.

B. Specific Comments

5. Accountability

The template recognises accountability as a GDPR principle but currently treats it similarly to the other Article 5 principles. Since accountability under Article 5(2) requires the controller not only to comply, but to be able to demonstrate compliance, the template could provide more explicit prompts on documentation, governance,

evidence, and review mechanisms.
In particular, both the template and the explainer generically invite to list the measures and discuss the appropriateness and the effectiveness of them. No methodology is provided. We recommend the template to provide examples of indicators, to make accountability more measurable and comparable across organisations.

6. Lawfulness of data processing

The template requires the controller to reflect on a legal basis for data processing (Section 2.1.a) and, if applicable, on reasons to lift the prohibition of the processing of the special categories of personal data (Section 2.1.b). While the adherence to the GDPR's principle of lawfulness is essential to ensure that data processing respects the fundamental right to personal data protection enshrined in Article 8 of the EU Charter, the way Sections 2.1.a and 2.1.b of the consulted template have been designed resembles a tick-box exercise rather than a demand for a thorough examination of compliance with Article 6 and Article 9 of the GDPR. Given the specificity of every legal ground for the processing of personal data and reason to lift the prohibition of the processing when special categories of personal data are concerned, it would be desirable that the template accounts for these specificities and relevant requirements. Therefore, we recommend the template to provide a separate table (or additional rows in the current table) for every legal basis (Article 6(1) GDPR) and every reason to lift the processing prohibition (Article 9(2) GDPR) individually. While the choice of every legal basis or reason to lift the prohibition requires a careful scrutiny, the steps of which should be explained in the DPIA, two points merit special attention, namely consent of the data subject and legitimate interest of the data controller or a third party.
When the controller requests data subject's consent for the processing (Article 6(1)(a) and Article 9(1)(a) GDPR), the table in the template should require the controller to check if and explain how all compulsory requirements of consent have been fulfilled. We recommend that the template includes a space, where the controller elaborates on how the conditions set out in Article 7 of the GDPR are satisfied, as well as how the inherent features for consent (freely given, specific, informed, unambiguous, and – for the special categories of data – explicit) are preserved. Furthermore, considering increasingly prevalent risks posed by information society services to minors, we strongly recommend that the template takes explicit account of the requirements for consent of the children obtained in line with Article 8 of the GDPR. In particular, we advise that the template provides space to explain how the controller handles age verification and what efforts are undertaken to anticipate and avert risks to minors, which the services in question may entail.
Where the controller relies on the legal ground for data processing formulated in Article 6(1)(f) of the GDPR, i.e. on the legitimate interest of the controller or a third party, we recommend that the template clearly sets out the relevant requirements and demands explanation of every step of the assessment. Instead of merely referring to the EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR in a footnote, we propose to structurally separate a space in the template, where the controller explains how the "three-step assessment" proposed by the EDPB has been performed. In doing so, the template can follow the logic of the Guidelines and request elaboration on each of the steps, i.e.:

- 1st step: Pursuit of a legitimate interest by the controller or by a third party
- 2nd step: Analysis of the necessity of the processing to pursue the legitimate interests
- 3rd step: Methodology for the balancing exercise.

To balance the need for maintaining clarity of the template and the necessity to provide explanation of the specific elements of the risk assessment, we propose to add references to relevant parts of the EDPB Guidelines 1/2024, where the controller can seek further explanation on the steps of the evaluation of the legitimate interest.

7. Necessity and proportionality

Traditionally, the *lato sensu* proportionality test is constructed as comprising three sequential sub-tests: suitability, necessity, and proportionality *stricto sensu*. In keeping with the EDPS necessity toolkit and proportionality guidelines, the EDPB's DPIA template (sections 3.2 and 3.3) focuses on necessity and proportionality. The template considers the suitability test ("*Evaluate if the envisaged processing is effective*") as part of the necessity test. We

suggest amending the template so that it reflects the tripartite structure of the proportionality test, so that it has three separate sections for suitability, necessity, and proportionality *senso strictu*. Before assessing whether the processing is the least restrictive measure that is still suitable for the achievement of the objectives set by the controller (necessity), and whether its benefits outweigh the interference it entails, data controllers should evaluate whether that processing is suitable, i.e. whether it pursues a proper purpose in the EU legal order, and whether its means are rationally connected to the goals it aims at achieving, *inter alia* in line with what is required by the purpose limitation principle.

More generally, Sections 3.2 and 3.3 could benefit from additional practical guidance and examples illustrating how controllers are expected to document necessity and proportionality assessments.

8. Security of personal data processing and personal data breaches

The template requires the data controller to reflect on the measures supporting the security of processing, the measures that are or will be implemented as well as their appropriateness and effectiveness (Section 2.3.e). As the CJEU noted in the *Natsionalna agentsia za prihodite* case, the appropriateness of technical and organisational measures implemented pursuant Article 32 GDPR is to be assessed in practice. The assessment encompasses both the nature and the content of the measures, the manner in which they are applied, as well as the practical effect on the level of security. The human factor remains a great risk when it comes to cybersecurity and the security of personal data. We propose that the template clarifies that both technical (e.g. encryption) as well as organisational (e.g. access rights policies, policy for passwords, training and awareness campaigns for employees) measures are to be implemented pursuant Article 32 GDPR.

Strengthening cybersecurity and the security of personal data is a continuous process. Rather than a one-time tick-box exercise, the security of personal data requires continuous attention and the proactive monitoring of the changing threat landscape, its impact on the risk assessment, and adapting the appropriate technical and organisational security measures to be implemented accordingly. We propose that this continuous element of assessing and implementing the appropriateness of security measures is added to the proposed DPIA template.

It is important to recall that not only the data controller but also the data processor is subject to the obligation to implement appropriate technical and organisational security measures pursuant Article 32 GDPR. From the controller's perspective, security considerations must be taken into account in the selection of the processor. Moreover, the GDPR requires that a processing agreement is in place between the data controller and data processor(s). As stipulated in Article 28(3)(c) GDPR, security measures are an important component of such a processing agreement. The processing agreement should include concrete information regarding how the GDPR's requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement. In its Guidelines 07/2020 on the concepts of controller and processor in the GDPR, the EDPB further specified the respective roles of the controller and processor when it comes to the GDPR's security requirements. The EDPB Guidelines detail what should be included in the contract with regards to security measures, including 'the security measures to be adopted, an obligation on the processor to obtain the controller's approval before making changes, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The EDPB guidelines advise documenting at minimum the necessary technical and organisational measures in the contract. The controller exercises its decision-making power over the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor. The proposed DPIA template could be improved with regards to the security of processing by making reference to the role of the data processor for implementing technical and organisational security measures and the processing agreement. The EDPB 07/2020 guidelines are useful for clarifying the respective roles of the controller and processor when it comes to the security measures. Overall, we propose that this is more clearly reflected in the proposed DPIA template.

Despite technical and organisational security measures, personal data breaches may still occur. Such personal data breaches may in some circumstances trigger notification requirements as stipulated in Article 33 and Article 34 GDPR. In any event, pursuant to Article 33(5) GDPR the data controller is obliged to document any personal data

breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. We propose adding to the template the setting up of such an internal or register or documentation for personal data breaches by the data controller.

***

TILT remains at the European Data Protection Board's disposal should it require further information or clarification on the present submissions.

All communications related to this document could be directed to Dr. Marco Bassini via the email address provided herein: m.bassini@tilburguniversity.edu

Contributors:
Dr. Marco Bassini
Dr. Lorenzo Dalla Corte
Dr. Magdalena Brewczyńska
Dr. Sofia Santinello
Mr. Suzanne Nusselder

Tilburg (Netherlands), 9 June 2026