Romanian Academy
Legal Research Institute
Center for European Legal Studies

To:

European Data Protection Board

Contribution to the
EDPB DPIA template

Prof. Daniel-Mihail Șandru, PhD, Senior Researcher I (coordinator)
Daniela Duta, PhD Candidate, Associate Researcher (rapporteur)
Marius Cătălin Mitrea, PhD Candidate, Scientific Researcher

Romanian Academy
Legal Research Institute
Center for European Legal Studies

EDPB DPIA template
Public consultation

INTRODUCTION

The Legal Research Institute, Centre for European Legal Studies, welcomes the initiative of the European Data Protection Board to develop a common template for Data Protection Impact Assessments (DPIAs). A harmonized approach to DPIAs has the potential to enhance legal certainty, facilitate consistent implementation of Article 35 GDPR across Member States, and support organizations in identifying and mitigating risks to the rights and freedoms of natural persons.

At the same time, any common DPIA framework should preserve the flexibility inherent in the risk-based approach established by the GDPR. The purpose of a DPIA is not merely to document compliance, but to provide a meaningful assessment of the necessity, proportionality, and risks associated with a specific processing operation. Excessively detailed or prescriptive documentation requirements may shift the focus from substantive risk assessment to formal compliance exercises.

In this respect, the proposed DPIA Template should remain a voluntary and non-binding reference framework that supports entities in meeting their obligations under Article 35 GDPR. It should not be interpreted as imposing additional legal obligations beyond those established by the GDPR, nor should it prevent from relying on alternative methodologies or internal governance frameworks capable of achieving equivalent levels of accountability and protection.

Furthermore, consideration should be given to the increasing interaction between GDPR compliance obligations and other regulatory frameworks, particularly Regulation (EU) 2024/1689 (AI Act). To avoid unnecessary duplication and administrative burden, the DPIA Template should facilitate interoperability with existing compliance instruments, including Records of Processing Activities (RoPAs), Transfer Impact Assessments (TIAs), security assessments, and Fundamental Rights Impact Assessments (FRIAs).

The following observations and proposed amendments aim to strengthen the practical usability, proportionality, and legal clarity of the proposed DPIA Template while preserving its objective of promoting a consistent European approach to data protection impact assessments.

GENERAL REMARKS

The initiative of the European Data Protection Board to develop a common Data Protection Impact Assessment Template represents an important contribution towards greater consistency and harmonisation in the application of Article 35 GDPR throughout the European Union.

At the same time, several aspects of the draft template would benefit from further refinement.

First, the final template should preserve the flexibility inherent in the GDPR's risk-based approach and avoid creating the perception of a mandatory or exhaustive compliance framework. Controllers should remain free to adopt alternative methodologies capable of achieving equivalent levels of accountability and protection.

Second, the template should place greater emphasis on methodology and risk assessment techniques rather than extensive documentation requirements. Harmonisation is more effectively achieved through common analytical approaches than through highly prescriptive reporting structures.

Third, duplication with existing compliance instruments should be reduced. Cross-references to Records of Processing Activities, Transfer Impact Assessments, security assessments, processor-management documentation, and other governance instruments should be expressly permitted where appropriate.

Fourth, greater clarity should be provided regarding the expected level of granularity throughout the template, particularly in relation to personal data categories, processing purposes, retention periods, data quality metrics, risk scenarios, and mitigation measures.

Fifth, the template should be further aligned with the evolving European digital regulatory framework, including Regulation (EU) 2024/1689 (Artificial Intelligence Act) and Fundamental Rights Impact Assessments, to minimise duplication and promote regulatory coherence.

Finally, additional practical guidance, examples, and methodological explanations would significantly improve the usability of the template and support consistent implementation by controllers of different sizes, sectors, and levels of organisational maturity.

A balanced approach combining harmonisation, proportionality, accountability, and operational flexibility would best support the dual objective pursued by the GDPR: facilitating responsible innovation while ensuring effective protection of the fundamental rights and freedoms of individuals.

Key points:

1. **Voluntary Nature of the DPIA Template**

Observation: The draft DPIA Template repeatedly emphasises the objective of achieving harmonisation among supervisory authorities. While this objective is legitimate and desirable, there is a risk that the template may gradually become a de facto mandatory standard despite being formally presented as a voluntary instrument.

Proposed Amendment: The EDPB should explicitly clarify that:

(a) the DPIA Template constitutes a non-binding reference tool adopted pursuant to GDPR and art. 9.2 EDPB - EDPS Joint Opinion 2/2026;

(b) controllers remain free to use alternative methodologies and documentation structures, provided that the substantive requirements of Article 35 GDPR are fulfilled.

Justification: The GDPR establishes a risk-based approach rather than a prescriptive documentation model. Excessive standardisation may undermine the flexibility required to assess diverse processing operations across different sectors and organisational contexts.

2. **Proportionality and Administrative Burden**

Observation: Several sections of the template require a level of detail that may exceed what is necessary to demonstrate compliance with Article 35 GDPR. In practice, the completion of all sections at the level of granularity suggested by the template could result in extensive documentation exercises with limited additional value for risk assessment.

Proposed Amendment: The template should distinguish between:

- mandatory minimum information necessary for every DPIA;

- optional information that may be included where justified by the nature, scope, context, and purposes of the processing.

Justification: The principle of proportionality requires that compliance obligations remain appropriate to the risks involved. DPIAs should focus on identifying and mitigating risks rather than generating excessive documentation.

3. Avoidance of Duplication

Observation: The template requires information that is frequently already maintained through other GDPR compliance instruments, including:

- Records of Processing Activities (RoPAs);
- Transfer Impact Assessments (TIAs);
- security documentation.
- processor management documentation and internal governance frameworks.

Proposed Amendment: The template should expressly permit controllers to refer to existing documentation through cross-references instead of reproducing identical information.

Justification: Allowing cross-references would reduce administrative burden, improve consistency across compliance documents, and decrease the risk of contradictory information appearing in different records.

4. Alignment with the AI Act

Observation: The increasing interaction between the GDPR and Regulation (EU) 2024/1689 (Artificial Intelligence Act) creates potential overlaps between DPIAs and Fundamental Rights Impact Assessments (FRIAs).

Proposed Amendment: The EDPB should include guidance explaining:

- the relationship between DPIAs and FRIAs.
- circumstances where information generated for one assessment may be reused for the other.
- mechanisms for avoiding duplication of assessments.

Justification: Controllers deploying high-risk AI systems may otherwise be required to perform substantially similar assessments multiple times. Regulatory coherence would improve legal certainty and compliance efficiency.

5. Need for Greater Methodological Guidance

Observation: The template focuses primarily on documenting information rather than explaining how controllers should assess necessity, proportionality, likelihood, severity, and risk acceptability.

Proposed Amendment: The EDPB should supplement the template with practical examples, case studies, methodological guidance regarding risk assessment, examples of acceptable mitigation measures.

Justification: Harmonisation is more likely to be achieved through common methodologies than through highly detailed documentation requirements. Additional methodological guidance would improve consistency among controllers and supervisory authorities.

6. Consistency of Risk Terminology

Observation: The concepts of likelihood, severity, inherent risk, residual risk, and risk to the rights and freedoms of data subjects are not always defined with sufficient precision.

Proposed Amendment: The EDPB should introduce a common taxonomy and risk language applicable across:

- DPIAs.
- personal data breach assessments.
- prior consultation procedures.
- AI-related risk assessments where relevant.

Justification: Consistent terminology would facilitate comparable risk assessments across Member States and reduce interpretative uncertainty.

7. Clarity Regarding Granularity Requirements

Observation: Several sections of the template do not clearly specify the expected level of granularity. This issue is particularly relevant regarding:

- personal data categories.
- processing purposes.
- retention periods.

data quality requirements.

Proposed Amendment: The EDPB should provide examples illustrating the expected level of detail and clarify whether information should be documented:

- by category of data.
- by processing activity.
- by individual data element.

Justification: Without such clarification, organisations may adopt inconsistent approaches, thereby undermining the harmonisation objective pursued by the template.

8. Risk Assessment and Management

General Observation: The risk-assessment section constitutes the core of the DPIA process. However, the proposed template introduces several methodological concepts whose practical relationship remains insufficiently defined.

In particular, the distinction between:

- inherent risks.
- risks arising from abnormal events.
- mitigated risks.
- residual risks.
- requires further clarification.

Without additional guidance, different controllers may adopt substantially different methodologies, thereby undermining the objective of harmonisation pursued by the template.

9. Impacts on Rights and Freedoms Caused by Non-Default, Accidental, Unlawful or Abnormal Events

Observation: The template requires controllers to identify threats arising from malfunctions, cybersecurity incidents, human error, unlawful access, unauthorised disclosure, and other abnormal events.

While these risks are important, they overlap swith traditional information-security risk assessments conducted under Article 32 GDPR, NIS2 and DORA obligations, cybersecurity frameworks, and internal security governance processes.

Proposed Amendment: The template should:

(a) clarify the relationship between DPIA risks and cybersecurity risks.

(b) allow references to existing security assessments.

(c) avoid requiring duplication of detailed security documentation.

Justification: Cybersecurity risk management and data protection risk management are closely related but not identical. Controllers should be encouraged to build upon existing security assessments rather than reproduce identical analyses within multiple compliance documents.

10. Method

Observation: The template requests an explanation of the methodology used to assess risks, including likelihood, severity, prioritisation criteria, and risk-acceptance thresholds.

This section is particularly important because it determines the consistency and reliability of the entire DPIA process.

However, the template provides very limited methodological guidance and does not identify preferred approaches, minimum requirements, or illustrative examples.

Proposed Amendment: The EDPB should provide:

(a) a common glossary of risk concepts.

(b) examples of risk matrices.

(c) examples of likelihood and severity scales.

(d) examples of risk-acceptance criteria.

Justification: A common methodology would significantly enhance harmonisation and comparability between DPIAs conducted by different organisations.

11. Inherent Risk Assessment

Observation: The distinction between inherent risk and residual risk raises methodological questions. Traditionally, inherent risk refers to the level of risk before any mitigating measures are applied. However, many processing activities are designed from the outset with technical and organisational safeguards already integrated through privacy-by-design principles.

As a result, it is not always clear whether:

- inherent risk should be assessed before any safeguards whatsoever.
- planned safeguards should be considered.
- only implemented safeguards should be considered.

This ambiguity may lead to inconsistent risk calculations.

Proposed Amendment: The EDPB should explicitly distinguish between:

(1) inherent risk before safeguards.

(2) risk after planned safeguards.

(3) residual risk after implemented safeguards and additional mitigation measures.

Justification: Clear separation of these concepts would improve transparency, facilitate prioritisation of mitigation activities, and enhance consistency across risk assessments.

12. Action Plan

Observation: The action-plan section appropriately requires controllers to identify additional mitigation measures and reassess residual risks.

However, the template should place greater emphasis on continuous monitoring and review obligations.

Risk assessments are not static exercises. Technological developments, organisational changes, new data uses, AI deployment, regulatory developments, and emerging threats may alter risk profiles over time.

Proposed Amendment: The action plan should explicitly include:

a) review triggers.
b) reassessment intervals.
c) responsibilities for monitoring risk evolution.
d) criteria requiring DPIA updates.

Justification: The accountability principle under Article 5(2) GDPR requires ongoing evaluation rather than one-time compliance exercises. A dynamic review framework would better reflect the lifecycle nature of privacy risk management.

CONCLUSIONS

The development of a common European DPIA Template represents an important step towards greater consistency in the application of Article 35 GDPR across the European Union. The initiative can contribute to legal certainty, improve supervisory convergence, and support organisations in implementing effective data protection governance mechanisms.

Nevertheless, the proposed template would benefit from further refinement to ensure that it remains fully aligned with the principles of proportionality, accountability, and risk-based regulation underpinning the GDPR. Several sections currently require a level of

granularity that may create unnecessary administrative burden, duplicate information already contained in other compliance documents, and reduce the practical effectiveness of the DPIA process.

The final version of the template should therefore:

- remain a voluntary and flexible reference tool;
- allow the use of cross-references to existing compliance documentation;
- provide clearer guidance regarding the expected level of granularity;
- reduce duplication between different sections of the template;
- include additional practical examples and methodological guidance;
- ensure consistency with other EU regulatory frameworks, including the AI Act and Fundamental Rights Impact Assessments.

A balanced approach that combines harmonisation with operational flexibility would better support both compliance objectives and the effective protection of the fundamental rights and freedoms of data subjects.