

**Comments on the
European data Protection Board's DPIA Template**

European Federation of Data Protection Officers
June 2026

EFDPOs Position

Following the European Data Protection Board's (EDPB) request for public consultation on DPIA Template ("Template"), the European Federation of Data Protection Officers (EFDPO) takes this opportunity to contribute to the ongoing discussion with the following comments.

Our approach to the issues raised by this public consultation is that of a European umbrella association of data protection and privacy officers. The objective is to create a European network of national associations where information, experience and methods can be exchanged. We will establish a continuous dialogue with the political sphere, business representatives and civil society, to facilitate a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European legal acts and texts regarding privacy.

The EFDPO welcomes the EDPB's initiative to document a coherent view on the performance and the documentation of a data protection impact assessment. The WP248 has already provided very useful guidance for Data Protection Officers (DPOs) on this risk assessment. Regarding the current practice on DPIA the EFDPO would like to stress the importance of the following topics that have not been mentioned in either the WP248 or the template:

1. Harmonization and overlap with Art. 30 records and other documentation

- Comment: The template should explicitly acknowledge and leverage overlap between the DPIA and records of processing activities (Art. 30) to avoid duplicative work. Many controllers already document the same elements in multiple places. Allowing reuse reduces burden, supports consistency and auditability, and advances harmonization across the EU member states.
- Proposed guidance text in the templates explanation: "To minimize administrative burden, controllers may reuse and cross-reference information between the record of processing activities under Article 30 and the DPIA under Article 35, provided the information remains complete, accurate, and up to date. Where the same fields are required (for example, purposes, categories of data subjects and data, recipients, transfers, retention, and security measures), controllers may reference a single authoritative source rather than duplicating content."

2. Separation of threshold analysis

- Comment: Part of the DPIA is the threshold analysis. It should be integrated here or have a clear reference. Especially the identified Risks from the threshold analysis should be clearly considered during the DPIA.
- Rationale: Criteria indicating high risk (e.g., large scale, vulnerable data subjects, special category data, systematic monitoring, innovative technology,

matching/combining datasets, ADM/profiling) the high risk should be addressed during the analysis. We found that these risks get in the background when looking at measurements documentation etc.

- Proposed solution: Integrate the threshold template with clear identification for reference and highlight the necessity to explicitly address the identified risks.

Regarding the national authorities “blacklists/whitelists” under Art. 35(4) a clear list of the risks to be addressed for the specific kinds of processing activities would be of additional help.

3. Misleading „Scope“ section (1.1.d)

- Issue: The current wording could be read as allowing the controller to define scope purely at its discretion. It would be clearer to anchor scope in objective boundaries and links to authoritative records and artefacts with respect to the data protection impact assessment.
- Proposed guidance text: “Define the scope of the DPIA by reference to objective boundaries and the risk creating parts of the processing. Link to:
 - The corresponding Article 30 record(s) and processing-activity identifier(s)
 - System and application inventory entries
 - Data flow diagrams and architecture descriptions (including upstream/downstream systems, processors, and sub-processors)
 - transfer flows
 - In-scope and out-of-scope elements (e.g., datasets, functionalities, user groups) Controllers should avoid arbitrary scoping; the DPIA should cover the full processing operation as implemented, including relevant interfaces and dependencies.”
- Optional note: Encourage controllers to include versioned links to change requests, product requirements, and security/privacy design reviews to maintain traceability.

4. Unclear “Quality of data” section (2.2.b)

- Issue: The intent of “quality of data” is unclear and appears disconnected from the principles and legal requirements in data protection. If the purpose is to assess risk from poor data quality, it should be tied explicitly to GDPR accuracy (Art. 5(1)(d)) and related principles, or be renamed and placed within the necessity/proportionality and risk sections. But this is already covered in the following section (2.3). Even the explainer text does not help to comprehend the goal of the section, especially with respect to data protection.
- Proposed solution:
 - Rename to “Accuracy and data quality” and clarify its scope, or alternatively

- Integrate it under the necessity/proportionality assessment and risk assessment, so it is evaluated as a factor that can create or exacerbate risks to rights and freedoms.
- Proposed clarifying text: “Assess risks arising from inaccurate, incomplete, untimely, inconsistent, or unrepresentative data, and describe measures to address them, with reference to Article 5(1)(d) and Article 16. Where relevant (e.g., profiling or automated decision-making), consider representativeness and bias in datasets used, as well as validation and monitoring of outputs.”
- Suggested elements to cover could be named in the explainer:
 - Dimensions: accuracy, completeness, timeliness, consistency, integrity/lineage, representativeness (where modelling or profiling is used)
 - Risks: erroneous decisions or discrimination due to incorrect/outdated data; denial of rights or services; opacity that prevents rectification
 - Measures: input validation, source verification, deduplication, periodic reviews, human-in-the-loop checks for high-impact decisions, data provenance tracking, rectification workflows, data subject communication, retention practices to prevent staleness, monitoring and recalibration for models
 - Evidence: error rates, QA procedures, audits, and metrics; links to testing/monitoring artefacts

5. Significant overlaps and redundancy in the section documenting measures (2.3 and 4.2.a)

- Issue: section 2.3 is structured into five subsections. Single measures will contribute to various goals in multiple subsections. Subsections are also consisting of overlapping topics. This phenomenon can be thought of being laid out in the structure of the GDPR. E.g. the principle of integrity and confidentiality and the accuracy principle are detailed especially with Art 32. Therefore, if one will document measures one will have to name the same measures multiple times, as 2.3. consists of the principles and 2.3.d and e defines details of these principles. This also holds true for the transparency goal and 2.3.b detailing the rights of the data subjects. All in all we expect a highly redundant documentation with a hard to read result. The additional value in this repetition is limited.

Furthermore the documentation of risk mitigation in section 4.2.a is not linked to the already named and listed measures. With the current template the risk mitigation analyses seems unnecessarily fragmented.

- Suggestions:
 - First, 2.3 might be restructured following a list of a reduced number of coherent goals, thinking of the additional provisions of the GDPR detailing the principles of Art 5.

- A second approach to avoid the kind of problem is to use a matrix, where goals/principles are listed in one direction and measures in the other. One particular measurement can then contribute to multiple goals.
- The third idea which also is around in other templates is to have a list of measures first, with a numbering scheme and then listing the measures by reference.
- Other approaches document the risk/measurement analysis in an additional spreadsheet, where during the analyses the identified risks, already existing measures are documented first in a risk analyses process. The additional measures are then considered coherently to mitigate the remaining risks. We suggest to consider this slightly different approach to avoid the named issues.

Final remarks:

The EFDPO wants to stress that it welcomes this helpful guidance on how to document a DPIA very much, and acknowledges and agrees that this topic was identified as problem domain for harmonization across Europe and for practical relevance for controllers. From our membership we support that the topic was in enormous need of guidance.

EFDPO contacts:

EFDPO Press Office, phone +49 30 20 62 14 41, [email: office@efdpo.eu](mailto:office@efdpo.eu),

President: Thomas Spaeing (Germany)

Vice Presidents: Xavier Leclerc (France), Judith Leschanz (Austria), Inês Oliveira (Portugal), Vladan Rámiš (Czech Republic)

About EFDPO

The European Federation of Data Protection Officers (EFDPO) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The association is based in Brussels.

Members:

- Austria: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at
- Czech Republic: Spolek pro ochranu osobních údajů
- Finland: Finnish Data Protection Association (Tietosuojary)
- France: UDPO, Union des Data Protection Officer - DPO
- Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
- Greece: Hellenic Association for Data Protection and Privacy (HADPP)
- Hungary: Hungarian Association for Data Protection Awareness, MADAT (Magyar Adatvédelmi Tudatosságért Társaság Egyesülete)
- Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
- Norway: Norwegian Association of Data Protection Officers (in Norwegian: *Foreningen Personvernombudene*)
- Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
- Slovakia: Spolok na ochranu osobných údajov
- Switzerland: DAPRI Data Privacy Community