

Comments on the EDPB's Draft DPIA Template

These comments are submitted in a personal capacity and reflect only the author's views.

On 14 April 2026, the EDPB published its *Draft DPIA Template* for public consultation, together with an Explainer. The Draft appears intended to serve as the basis for a semi-official or official template to be used by “*all data protection authorities*”. Given the significance of that objective, it is submitted that both the Draft and the Explainer would benefit from further development and clarification before finalisation.

1. The document entitled “Explainer” is shorter than the document it is intended to explain (net 10 pages, as compared with net 15 pages) and, in a number of places, largely repeats the wording of the Draft (see, for example, points 0, 2, 3, 5, 7, 12, 15, 28 etc.). As a result, it presently offers only limited additional guidance.

2. The Draft may be suitable for a relatively simple data processing activity (for example, the assessment of a small database-like data processing activity), but it appears less well suited to a complex, multi-step process in which the purposes, data subjects, categories of relevant personal data, retention periods, and other conditions of the data processing may differ from one stage of the processing activity to another.

3. In several respects, the Draft and the Explainer read less like legally precise instruments than might be expected of documents of this importance. They use expressions that do not appear in the GDPR [for example, “illegitimate access, undesired modification and disappearance of data” instead of the terminology used in the definition of a personal data breach in Article 4(12) GDPR]. They also use the term “means” in a different sense (that is, as a tool—for example, Explainer point 20) from its established meaning in data protection law and practice (“purpose and means”, “essential and non-essential means”). Similarly, the term “operations” (cf. section 1.1.d of the Draft) appears to refer more specifically to “data processing operations”. With regard to risk, the Explainer (point 42) uses the phrase “unacceptable or excessively high risks” instead of the terminology used in the GDPR, etc.

4. The provisions concerning risks and mitigation measures would benefit from further clarification.

a) Risks are to be assessed in both Section 3.1 and Section 4. Even if one accepts the explanation in point 35 of the Explainer, an important question remains: what precisely distinguishes “inherent” risk from “residual” risk within the Draft? If mitigation measures (described in the Draft and the Explainer as “measures supporting compliance”) may already have the status of “planned”, the distinction between “inherent” and “residual” risk may lose practical significance. Any measure classified as an “additional” measure could equally have been included earlier as a “planned” mitigation measure before the inherent risk was determined. Moreover, if some mitigation measures are already taken into account when assessing the inherent risk, the effectiveness of the said mitigation measures cannot readily

be evaluated: one cannot know the level of risk before any mitigation measures were applied, and therefore cannot determine the extent to which those measures reduce the risk. The use of “modulating factors” (see Section 4.1.c) further complicates the analysis. Finally, it remains unclear what distinguishes mitigation measures under the various sections of the Draft from the “Conditions” referred to in Section 6.

b) Although the GDPR requires the controller to assess the risks to the rights and freedoms of natural persons arising from the processing of personal data, and those “rights and freedoms” are not limited to data protection rights (cf. WP 248 rev.01, p. 6), the Draft and the Explainer appear to focus primarily on data protection rights. In that regard, it is noteworthy that neither document expressly requires the controller to consider which rights and freedoms may be affected by the processing activity.

c) In addition, the Draft and the Explainer may give the impression that, by “risk”, they primarily refer to IT security risks, rather than the broader range of relevant risks.

d) It is also not entirely clear why the Draft refers to the “method” for assessing risks only in Section 4.1.b. It would be helpful to clarify what method is intended to apply under Section 3.1.

5. Additional comments on the Draft and the Explainer:

a) Neither the Draft nor the Explainer provides guidance on whether additional rows or multiple charts may be added to the template (for example, in Section 1.1, depending on the complexity of the processing activity). As currently drafted, one might infer that all information must be confined to the space provided, even where the complexity of the processing would call for a different approach.

b) The Draft combines substantive content with references to external sources in a manner that may benefit from greater consistency. For example, it is not immediately apparent why the section on the “Reasons to conduct the DPIA” (Section 0.5) requires a detailed repetition of the so-called threshold assessment, while in many other instances the Explainer (for example, paragraphs 10, 14, and 23) appears to regard a reference to other documents as sufficient.

c) Section 0.3 appears to suggest that the record of processing activities (RoPA) is the starting document in the design of a processing activity, whereas, in practice, it should more appropriately be the final document. A RoPA merely describes the conditions of a processing activity; it does not create or constitute them.

d) Section 5 appears to suggest that the DPO (if one exists) provides an opinion before consultation with the representatives of the data subjects, even though the DPO may itself recommend such consultation. It is also unclear whether Section 5.1 is intended to contain only the controller’s summary of the DPO’s opinion and the measures to be taken in response, or whether the DPO’s opinion is to be attached to the DPIA without amendment.

6. Neither the Draft nor the Explainer appears to address the possible interplay between the DPIA and the AI Act, namely when a Fundamental Rights Impact Assessment may also be required.

* * *

In light of the above comments and observations, I am concerned that the Draft and the Explainer are not, in their current form, suitable to serve as a template unless they are thoroughly redrafted, preferably with the support of data protection practitioners who have already carried out a DPIA.

Zsolt Bartfai