RESPONSE TO THE PUBLIC CONSULTATION
OF THE EUROPEAN DATA PROTECTION BOARD

/on Data Protection Impact Assessment template/

9 June 2026

Regulation (EU) 2018/1725 provides rules for the processing of personal data by EU institutions, bodies, offices and agencies. The principles of personal data protection laid down in Regulation (EU) 2018/1725 are identical to the GDPR and the co-legislators decided that they must be interpreted homogeneously with it[1]. In this context, given that the adoption of a DPIA template by the EDPB will have an impact on the way in which European institutions, bodies, offices and agencies conduct data protection impact assessments, a group of data protection officers of several EU institutions, bodies, offices and agencies, agreed to provide the following comments in response to the public consultation of the EDPB on DPIA template:

(1) Section 0.2: the **early identification of processing locations** of processors and sub-processors as an indicator of potential international transfers could help the organisations to identify transfers-related risks early.

(2) Section 0.5: a question that assesses **the need to conduct a DPIA** could result in duplication of administrative effort. In line with the principle of accountability, controllers are required to demonstrate (and by consequence – to document) their assessment on the need to carry out DPIA for each processing operation. Should the EDPB template include detailed analysis on the need to conduct DPIA in the DPIA template, controllers will have to either fill the DPIA for every processing operation or will be required to duplicate this information from another documentation. An alternative approach could be considered – to reference the document that concludes on the need to carry out a DPIA. Furthermore, compliance structures in organisations would benefit from a clear description of a governance model (e.g., RACI) for the DPIA accountability and lifecycle management.

(3) The clear definition of scope, including what is considered out of scope, would contribute to completeness of the assessment. Such clarification is necessary to ensure that DPIAs provide a complete and coherent representation of the

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, recital 5.

processing activity, while preventing gaps or inconsistencies in the assessment. Requiring controllers to define both the 'included' and the 'excluded' scope, together with the underlying rationale, would enhance transparency and traceability. Section 1: high-level description of the processing would benefit from clear **categorisation of personal data and data subjects**. The taxonomy of the essential elements of processing operation (data subjects, personal data, etc.) in the template would allow to clearly describe the processing operation in the context of which the DPIA is to be carried out. Additionally, categories of data subjects should be clearly defined and separated from the question on overall context of the processing, since processing of personal data of vulnerable or public data subjects (or personal data related to criminal convictions or data concerning health) could result in varying risk levels. The document would benefit on the development of a centralised taxonomy library of personal data types systematically linked to contextual processing fields and associated risk levels, to support DPIA practitioners in efficiently identifying and assessing risks based on the specific context of the processing operation.

(4) Section 1.1.c: The current guidance could be reinforced in respect to the requirement to perform a compatibility assessment for **further processing of personal data**, clarifying the definition of applicable technical and organisational safeguards or establishing links between safeguards, specific secondary use scenarios and associated risks.

(5) Section 1.2: functional **description of the processing must cover the whole lifecycle of data processing**. The template and explainer document would benefit from guiding controllers to provide a high-level description of the whole data lifecycle: from the moment of data collection (generation) to data destruction. The data flow mapping based on diagrams and life cycle description would ensure better transparency of processing operations.

(6) Section 1:3: considering the increasing complexity of IT systems and infrastructures supporting processing activities, the template should allow for a more structured description of the **asset inventory**, including systems, applications, infrastructure components, aligned with and proportionate to the risk assessment needs. In that context, several examples in the explainer or questions in the template could be introduced, including regarding the AI systems.

(7) Section 2.1: the template would benefit from **clearer mapping between the legal basis and processing steps** to prevent gaps and demonstrate operational lawfulness.

(8) Section 2.2: retention periods must clearly **define the trigger to start counting retention period**. Inclusion of structured guiding questions would contribute to ensuring a more substantive assessment (not only descriptive justification).

(9) Section 2.3.a: the description of **measures to support compliance with the principles** of data processing could be improved to include operational and practical examples. The explainer document that accompanies the DPIA template is unlikely to equip controllers with examples of the measures they could put in place to support compliance with the principles of data processing. In that respect, the template or the explainer document could refer to the guidelines with the relevant information, e.g., section 3 of the EDPB guidelines on data protection by design and by default.[2]

(10) Section 2.3.b: similarly to the point above, **the description of measures to support exercise of data subject rights** would benefit from inclusion of or referencing to the operational examples. Without them, it may be challenging for controllers to fill-in the template and for DPOs to advise on the measures to be put in place from the data subject rights' perspective. In addition, the assessment should be carried out for each right individually, also considering non-applicability of data subject rights in specific situations.[3] The template should include a field to reference restriction decisions where relevant.

(11) Section 2.3.c: the description of measures supporting **compliance with Article 28 of the GDPR** could benefit from further details to provide DPOs with the necessary information to advise. As the template stands now, it may be challenging to understand whether the data protection agreement is in place and to what extent its provisions comply with the requirements of Article 28. It may be appropriate to include more targeted questions in the DPIA template, for instance, on whether the standard contractual clauses[4] are included in the contractual framework, or in the absence of the standard contractual clauses – the checklist based on paragraph 3 of Article 28 of GDPR could help in carrying out the assessment.

(12) Sections 1.1.d and 2.3.c: identification of **international transfers** and description of safeguards could be reinforced. While DPIA and transfer impact assessment (TIA) are two separate assessments, the overview of to-be-

[2] EDPB guidelines 4/2019 on Article 25 – Data protection by design and by default

[3] For example, right to object Article 21(1) applies in case processing of personal data is based on points (e) or (f) of Article 6(1).

[4] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

transferred data, purposes and destinations of transfers and legal basis (under Chapter V of GDPR) supports identification of risks to the rights and freedoms of data subjects. It may be opportune to consider incorporation of essential TIA elements in the DPIA template. A structured transfer mapping (data, recipients, countries, purposes, safeguards) and explicit confirmation of TIAs would establish clearer description of international transfers.

(13) Section 2.3.e: description of the **measures supporting security of processing** would benefit from referencing concrete operational examples or international standardisation frameworks that provide a 'catalogue' of measures that controllers and organisations could put in place.

(14) Sections 3.2 and 3.3: more **targeted questions for assessment of necessity and proportionality** could increase consistency of the analysis across processing operations in a single organisation. While the template provides references to the necessity toolkit and proportionality guidelines, this may not be operational enough for controllers. A set of specific questions, for example *"What alternatives to processing personal data have been considered?"* and *"Why the alternatives have been disregarded?"*, could lead to improving quality and consistency of assessments in organisations.

(15) Section 4: **risk assessment** would benefit from consolidation. The risk scale, impact, likelihood must be clearly defined. Even it is a responsibility of controllers to define and document the risk assessment methodology, the identification and scoring of risks is unlikely to lead to effective mitigation of the risks if the template does not reference the methodologies or relevant parts of international standards for risk management and impact assessments[5]. Both, controllers and DPOs, could benefit from referencing methodologies describing examples of real-life effects on individuals in case the risk materialises (e.g., in case of a data breach). Each identified risk should be referenced once, and its treatment should be described in the same part of the template. Additionally, references to repositories of risk mitigation measures could help organisations to treat identified risks in a more consistent manner. Establishing links between risks and operational mitigation measures (including contractual controls) would equip controllers with the necessary tools to mitigate the risks.

(16) Lastly, it may be appropriate to **nuance publication of DPIA**. In some cases, publication of DPIA may serve public or legitimate interests of controller. In other cases – publication of certain parts of DPIA may compromise the security of

[5] See ISO/IEC 29134

personal data processing. In that context, it may be appropriate to consider marking of individual chapters / questions for publication rather that determining publication of the whole document. This could be easily achieved with the colour coding according to the level of information sensitivity (green / red) or providing guidance on how to prepare a summarised version for publication.

Overall, we welcome the efforts of the EDPB to prepare flexible DPIA template that different actors could adopt and adapt. At the same time, one of the DPO tasks is to advise controllers, who often face operational challenges in ensuring and documenting compliance. For that reason, the template should be reinforced with practical information and operational examples to improve the quality of information controllers include in DPIAs. This in turn would allow DPOs to provide more relevant advice and data protection authorities to supervise in a more efficient manner.

Data protection officers of the:

- European Parliament
- Council of the European Union
- European Economic and Social Committee
- Community Plant Variety Office
- European Banking Authority (acting DPO)
- European Medicines Agency