CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 20 7367 3000

cms.law

8 June 2026

Position on the European Data Protection Board Template [2026] for Data Protection Impact Assessment

CMS Cameron McKenna Nabarro Olswang LLP would like to thank the EDPB for the opportunity to provide comments on the Template [2026] for Data Protection Impact Assessment ("**Template**"). We welcome the EDPB's initiative to engage with stakeholders and promote a practical, consistent approach to DPIAs that supports effective accountability and risk assessment under existing Member State data protection frameworks. Our response reflects our experience in supporting our clients worldwide in preparing data protection assessments within existing regulatory frameworks. We remain at the EDPB's disposal should they have any questions.

EXECUTIVE SUMMARY

We support the objective of a practical and consistent DPIA that helps data controllers to identify, assess and mitigate risks to data subjects. We welcome that the Template addresses key elements of a DPIA from this perspective, including the reasons to conduct a DPIA, the nature, scope and context of the data processing, measures supporting compliance, impacts of the processing on the rights and freedoms of data subjects, and risk assessment and management. We propose that the Template should be applied in a proportionate and risk-based manner, in line with the requirements of Article 35 of the GDPR. In doing so, it may be helpful to ensure that the DPIA does not evolve into a technical, contractual, or operational catalogue extending beyond what is necessary to assess the risks associated with a proposed data processing.

Our comments address the following issues:

Section 0.1 (Data controller identification): The requirement to identify internal management units responsible for the data processing may go beyond the obligations set out in Articles 30 and 35 of the GDPR and could create some ambiguity regarding the meaning of "party" in the Explainer.

Section 0.2 (Data processors and sub-processors): The requirement to define the obligations and tasks of data processors and sub-processors within the DPIA may partially overlap with the documentation requirements already established under Article 28(3) of the GDPR.

Section 0.5 (Scope of the DPIA): The Scope field may be interpreted as introducing a requirement to justify excluded data processing activities, whereas it may be more focused on clearly describing the in-scope processing activities.

CMS Cameron McKenna Nabarro Olswang LLP is a limited liability partnership registered in England and Wales with registration number OC310335.
Notice: the company does not accept service by email of court proceedings, other processes or formal notices of any kind without specific prior written agreement.

Section 0.5 (Publication of the DPIA): Article 35 of the GDPR does not require publication or external sharing of DPIAs, and it may be helpful to ensure that the Template does not inadvertently suggest such an expectation.

Section 1.1.c (Secondary or compatible uses): The compatibility assessment under Article 6(4) of the GDPR is a standalone requirement and may not need to be fully reproduced within the DPIA.

Section 1.3 (Supporting assets and architecture): The current framing and examples may be understood as encouraging a highly granular level of IT asset documentation, which could be seen as overlapping with technical security inventories beyond what Article 35 of the GDPR requires.

Section 2.1.a (Legal basis - legitimate interest): The legitimate interest balancing test under Article 6(1)(f) of the GDPR is typically documented as a separate assessment and may not need to be replicated in full within the DPIA.

Section 2.2.b (Data quality): Rather than requiring fixed quantitative metrics for each data element, data quality could be assessed in a more contextual manner, focusing on accuracy, relevance, and appropriate updating mechanisms.

Section 2.3.c (GDPR Article 28 compliance measures): Including detailed Article 28 compliance (supporting) measures within the DPIA may partially duplicate information already covered in data processing agreements and related documentation.

DETAILED COMMENTS

We provide the following, more detailed comments on specific areas where further clarification would improve the Template's proportionality, workability and alignment with existing obligations under the GDPR.

1. Avoiding over-specification of internal organisational responsibilities in DPIAs

In Section 0.1, the Template requires identification of "*management units responsible for the processing inside the organisation*," whereas the GDPR does not explicitly impose an obligation - either externally or internally - to document internal organisational units responsible for a specific data processing activity. This may extend beyond the record-keeping requirements set out in Article 30 of the GDPR and could risk blurring the distinction between organisational governance documentation and the DPIA. In addition, the Explainer requires controllers to "*clearly define each party's obligations and tasks*", without clearly specifying whether "*party*" refers to the controller entity itself, joint controllers, internal management units, contact persons, representatives, or the Data Protection Officer. This lack of clarity may lead to different interpretations and potential legal uncertainty in implementation. It may therefore be helpful to clarify that the DPIA should focus on identifying the data controller (and joint controllers, where applicable) for accountability purposes, in line with the requirements of the GDPR, rather than requiring a mapping of internal organisational structures or reporting lines. This would help ensure that the DPIA remains focused on its primary function as a risk assessment tool, while avoiding unnecessary complexity or overlapping with internal governance documentation.

2. Avoiding duplication with Article 28 of the GDPR

In this section, we provide certain observations on potential overlaps between the DPIA Template and existing GDPR documentation requirements, in particular regarding data processor-related information under Article 28 of the GDPR, compatibility assessments under Article 6(4) of the GDPR, the treatment of legitimate interest assessments, including their relationship with DPIAs, and the extent of GDPR Article 28 compliance detail expected within the DPIA.

2.1 Clarifying the treatment of processor information under Article 28 GDPR in DPIAs

Section 0.2 (*Processor(s) and sub-processor(s)*) of the Template requires data controllers to identify data processors and sub-processors with, according to the Explainer, an "*unequivocal definition of their obligations and tasks*". While we understand the objective of ensuring transparency regarding the involvement of data processors and sub-processors, this requirement may inadvertently create a parallel documentation obligation that overlaps with the requirements already set out in Article 28(3) of the GDPR. (Under Article 28(3), data processing agreements are required to specify the subject matter, duration, nature and purpose of the processing, the type of personal data, the categories of data subjects, and the respective obligations and rights of the controller.) In this context, requiring data controllers to reproduce the same information within the DPIA may result in unnecessary duplication and additional administrative effort without providing significant added value from a risk assessment perspective. It may therefore be helpful to clarify that the Template should focus on those aspects of the processor relationship that are relevant to the assessment of risks and safeguards (for example, whether appropriate contractual, technical, and organisational measures are in place), rather than repeating information that will be documented and governed through GDPR Article 28-compliant contractual arrangements.

2.2 Avoiding duplication with Article 6(4) GDPR compatibility assessments

Documenting secondary or compatible uses, as well as assessing their compatibility, is already a requirement under Article 6(4) of the GDPR, which data controllers are expected to carry out irrespective of the DPIA. The GDPR does not expressly require that this assessment be reproduced within the DPIA itself. Against this background, including this element in Section 1.1.c (*Secondary or compatible uses*) of the Template may result in some duplication with the existing GDPR Article 6(4) compatibility assessment, or with information already maintained in the records of processing activities. It may therefore be helpful to ensure that the Template remains focused on its primary purpose as a risk assessment tool, while avoiding unnecessary repetition of documentation that is already required under the GDPR.

2.3 Avoiding duplication with Article 28 GDPR documentation in DPIAs

Section 2.3.c (*Relationship with processors*) of the Template includes a dedicated row requiring data controllers to document measures supporting compliance with Article 28 of the GDPR. While we appreciate the intention of ensuring that controller–processor arrangements are appropriately considered within the DPIA, requiring a detailed description of Article 28 compliance measures within the DPIA may lead to some duplication with information that must be set out in the data processing agreement. Instead, the Template could focus on confirming that an Article 28-compliant agreement will be in place with the relevant processor, and on identifying any residual risks arising from the processor relationship that are relevant to the specific processing operation under assessment.

2.4 Clarifying the relationship between LIAs and DPIAs under Article 6(1)(f) of the GDPR

The requirement to analyse legitimate interests and conduct a balancing test is derived from the Article 29 Working Party's Guidelines on Transparency (now endorsed by the EDPB) and forms part of the legitimate interest assessment (LIA) necessary to rely on Article 6(1)(f) of the GDPR. At the same time, the GDPR does not expressly require that this analysis be conducted within the DPIA itself. In practice, data controllers will often document their LIA as a separate exercise. Against this background, reproducing the full LIA within Section 2.1.a (*Legal basis*) of the Template may result in some duplication of documentation. It may therefore be sufficient allowing the DPIA to focus on the potential risk implications of the chosen legal basis for the rights and freedoms of data subjects.

3. Focusing on the relevant scope of processing rather than documenting excluded activities

The "*Scope of this DPIA*" field in Section 0.5 of the Template asks data controllers to identify "*what has been considered and what has been left out of the assessment and why*". While we appreciate the

intention of promoting transparency regarding the scope of the assessment, the current wording may be interpreted as requiring data controllers to document and justify all data processing activities that have been excluded from the DPIA. In practice, this could create a documentation burden that extends beyond what is necessary for an effective risk assessment.

From a data controller's perspective, it may be more helpful for the Template to focus on clearly defining the boundaries of the data processing operation under assessment, including the relevant personal data, purposes, systems, and data flows covered by the DPIA. Exclusions could then be addressed where there is a genuine ambiguity regarding scope, or where a related processing activity might reasonably be expected to fall within the assessment.

Such an approach would provide clarity regarding the scope of the DPIA while avoiding unnecessary documentation of data processing activities that are not relevant to the assessment. This would allow data controllers to focus their efforts on assessing and mitigating risks associated with the data processing activities that are within scope.

4. Ensuring that DPIA publication remains a voluntary practice under the GDPR

The inclusion of a field in Section 0.5 of the Template asking whether the DPIA "*is intended to be published or to be shared externally*" may be understood as suggesting that publication or external sharing is a common or encouraged practice. However, Article 35 of the GDPR does not require data controllers to publish or externally share DPIAs. In this context, the inclusion of a dedicated field on publication - particularly one that requires data controllers to actively select "No" alongside affirmative options - may inadvertently create the impression that publication is expected or represents a preferred approach. This could be challenging in practice, as DPIAs often contain trade secrets, details regarding security measures, internal risk evaluations, or other information that data controllers may reasonably decide not to disclose externally. It may therefore be helpful for the Template or Explainer to clarify that publication and external sharing of DPIAs remain entirely voluntary decisions for data controllers, to be assessed on a case-by-case basis. Such clarification would help avoid any unintended perception that choosing not to publish a DPIA reflects a lack of transparency or compliance, while still preserving the flexibility envisaged by the GDPR.

5. Avoiding overly granular or exhaustive infrastructure details

Section 1.3 (*Means of processing, supporting assets and underlying architecture*) of the Template asks data controllers to provide a detailed inventory of "supporting assets" and "underlying architecture", including - according to the Explainer - examples such as individual hardware components (servers, laptops, mobile devices, storage media, scanners, VPN gateways), specific software, APIs and models, personnel categories, and sites and premises. While the Explainer notes that "*very small, generic, or easily substitutable elements usually do not need individual listing*", the breadth of the examples provided may nevertheless be interpreted as encouraging a highly granular level of infrastructure documentation.

We appreciate the objective of ensuring that the processing environment is sufficiently understood to enable an effective risk assessment. However, it may be helpful to clarify that the level of detail expected should remain proportionate to the purpose of the DPIA and aligned with the requirements of Article 35 of the GDPR. A DPIA is primarily intended to assess risks to the rights and freedoms of individuals, rather than to serve as a comprehensive inventory of IT assets or technical infrastructure.

In practice, requiring extensive documentation of supporting assets and underlying architecture may create several challenges. First, it may blur the distinction between the DPIA and other forms of documentation, such as information asset inventories, security documentation, or system architecture records, which are often maintained separately. Second, it may increase the administrative effort associated with completing DPIAs without necessarily enhancing the quality of the risk assessment. Third, where DPIAs are shared internally or externally, a highly detailed description of infrastructure

components could raise concerns regarding the disclosure of sensitive security-related information. Finally, a strong focus on infrastructure details may risk diverting attention from the substantive assessment of data protection risks and mitigating measures, which lies at the core of the DPIA process. It may therefore be preferable for the Template to focus on a high-level description of the data processing environment that is sufficient to support the assessment of risks and safeguards, such as the categories of systems involved, and key data flows. Where more detailed technical information is necessary, data controllers could be encouraged to maintain such documentation separately and reference it as appropriate.

6. Data quality may be assessed in a risk-based and contextual manner

Section 2.2.b (*Data quality*) of the Template requires data controllers to provide "*quality metrics, requirements or thresholds*" for each processed personal data item. While we appreciate the objective of promoting data quality and supporting compliance with the accuracy principle under Article 5(1)(d) of the GDPR, the current wording may be interpreted as requiring data controllers to define quantitative metrics or fixed thresholds for every category of personal data.

In practice, such an approach may not always be feasible. Many data processing activities rely on information that is self-reported by data subjects or obtained from third-party sources, where the data controller's ability to establish or monitor specific quality metrics may be limited. Moreover, the appropriateness of a particular quality measure often depends on the nature of the data, the purposes of the data processing, and the potential impact of inaccuracies on affected individuals.

It may therefore be helpful to clarify that data quality should be assessed in a context-specific manner. In particular, the assessment could focus on whether the personal data is sufficiently accurate, complete, and relevant for the intended purpose; whether appropriate processes exist to maintain and update data where necessary; and whether data subjects can effectively exercise their rights to rectification and erasure.

Such an approach would remain aligned with the objectives of the accuracy principle while providing data controllers with the flexibility to adopt measures that are proportionate to the nature of the data processing. It would also help avoid situations where the establishment of formal metrics becomes an end in itself, rather than supporting the substantive goal of ensuring that personal data is fit for the purposes for which it is processed.

CONCLUSION

Overall, our position is that the Template should remain a practical tool for accountability, not a prescriptive checklist that requires unnecessary duplication of contractual materials, exhaustive technical inventories or quantitative metrics where they are not needed. A proportionate Template should focus on identifying the data processing activities, assessing the relevant risks to data subjects, documenting key safeguards, and supporting the data controller's decision-making. We therefore consider it important that the Template be clarified to ensure that data controllers can meet these objectives in a workable manner, in line with a risk-based application of Article 35 of the GDPR.

Emma Burnett
Partner | CMS Cameron McKenna Nabarro Olswang LLP