

PUBLIC CONSULTATION RESPONSE
EDPB Template and Explainer [2026] for Data Protection Impact Assessment (DPIA)
Version 1.0, adopted 10 March 2026

EXECUTIVE SUMMARY

We welcome the EDPB's initiative to provide a harmonised DPIA template. Our response raises practical concerns about clarity, operational workability, and avoidance of duplication with existing legal instruments. Executive summary provides a short overview of our key asks, while detailed comments include constructive practical suggestions and text improvement proposals. Our key asks are:

- **DPIA template shall be better connected to the explainer:** without reading the explainer in full the exercise seems simpler than it really is. We believe template shall contain key instructions for the user to be able to understand the expectations (in short and without examples) without reading the entire explainer.
- **DPIA template shall be more universal:** DPIAs can take place on different levels; process level, project level, system level etc. This template seems to be fit for a process level DPIA that cover only one processing activity.
- **Template sufficiency and non-redundancy (Comments 1, 2, 3):** Compliance with the template's content should explicitly satisfy Article 35 GDPR regardless of format. The "minimum" framing should be dropped. A completed template is a complete DPIA. Cross-referencing between sections and to external documents should be explicitly encouraged to reduce repetition across teams and documents.
- **Confirmation of mandatory elements & light DPIA (Comment 4):** Each section should be labelled mandatory (M), recommended (R), or contextual (C). A two-tier framework should distinguish full DPIAs from proportionate voluntary "light DPIAs." Graphical/schematic data flow description and asset inventory must be unconditionally mandatory in all cases; a DPIA lacking either shall be deemed incomplete regardless of trigger.
- **Non-duplication with other legal documents (Comments 5, 7):** Cross-references to Article 26 joint controller arrangements and Article 28 DPAs are sufficient, obligations and tasks of joint controllers and processors do not need to be reproduced in the DPIA.
- **Sub-processor listing and cascaded delegation (Comment 6):** Exhaustive sub-processor listing within the DPIA should not be required. General authorisation via pre-approved list under Article 28 SCC is legally sufficient and the DPIA should reference that mechanism. Cascaded DPIA delegation to processors, with collection of conclusions at controller level, should be explicitly recognised as a valid compliance model for complex multi-party chains. Processors should be required to transparently share data flows and asset inventories relevant to their segment, including transfer information.

- **DPO recommendation as DPIA trigger (Comment 10):** DPO recommendation under Article 39(1)(c) GDPR should be added as an explicit trigger alongside mandatory and controller-initiated assessments.
- **Governance and approval (Comments 9, 11):** RACI matrices should be referenceable from existing SOPs (when existing) rather than reproduced per DPIA; at minimum, names and roles of those directly involved should be recorded (but not the full RACI). Formal approval should be at an appropriate governance level per the controller's internal framework, defaulting to CEO sign-off is disproportionate and operationally unworkable at scale.
- **Secondary uses (Comment 12):** Secondary uses are separate processing activities and should not be embedded in the primary DPIA. The guidance should distinguish between secondary uses triggering their own DPIA including compatibility assessment; those requiring standalone compatibility documentation; and cases where none is contemplated. Linkage between parent and child activities belongs in records of processing activities.
- **Data flows as foundational element (Comment 13):** Section 1.2 must be unambiguously mandatory, covering all stakeholders, systems, countries of storage or transit, data sensitivity categorisation, and inter-system data movement. A DPIA without a documented data flow is incomplete in all circumstances.
- **Transitional arrangements (Comment 14):** Given the operational scale involved (large hospitals may maintain over 200 active DPIAs, clinical trial sponsors conduct one per trial) controllers should have two years from final publication to update DPIAs for ongoing processing, with immediate application only to new, significantly changed, or authority-directed processing.
- **Risk weighting of high-exposure processors (Comment 17):** The risk assessment should distinguish and weight the processors that drive risk considering main processors, those with ongoing access, and those handling special-category data, rather than treating all processors uniformly.
- **Technical measures and risk quantification (Comments 18–19):** Technical measures are under-represented, and the template offers no mechanism or clear methodology to quantify the risk score. A risk-scoring mechanism should enable controllers to evidence how technical and organisational measures reduce likelihood and severity, so the residual-risk conclusion is justified rather than asserted; assumption-based scoring should be expressly permitted for new processing.

About us:

MyData-TRUST is registered under Belgian Laws, active since 2017 in the data protection area and dedicated exclusively to the health and life science. Our multi-disciplinary team includes Data Privacy Lawyers, IT Security Specialists and Health data/Clinical Experts providing GDPR related services (such as privacy risk assessments, external DPO as a service, etc.). Our clients include among others Pharmaceutical, Biotech and Medical Devices companies, Contract Research Organisations (CROs), Healthcare providers and Health associations.

DETAILED COMMENTS

Comment 1 – Methodological flexibility should be preserved (p. 4)

Cited text: "Controllers can conduct their risk analysis and management processes as they prefer, using the DPIA **methodology of their choice** ..."

MDT view: This clarification is positive and important. In practice, organisations may rely on different established methodologies, such as CNIL, or internal risk-management frameworks which may also include ex-EU requirements (e.g. DPIA for a clinical trial run in EU & Canada).

Suggested improvement: This point should be kept and further emphasised. The final version should clearly state that the EDPB template is not intended to replace existing DPIA methodologies, nor shall it be deemed mandatory. It provides a common reporting and documentation structure acceptable to supervisory authorities (alongside other templates with similar content).

Comment 2 – Following the template shall be sufficient to document compliance with the Art. 35 GDPR (p. 4)

Cited text: " The EDPB template is one way to record the most important results, **a minimum amount of information** that should always be documented..."

MDT view: Framing the template as a "minimum" aside the reference to some simpler methodologies, such as the one of ICO, creates uncertainty for controllers. How far a simpler ICO template (cited in the document as a possible established methodology) would be sufficient, since it does not contain all the sections present in EDPB guidance? At the same time, it is unclear what additional information, or documentation may be expected by supervisory authorities beyond what the template captures (since what is in the template is the minimum), which undermines the harmonisation objective.

Suggested improvement: The EDPB should clarify whether compliance with the template and the explainer is sufficient for the purposes of Article 35 GDPR or explicitly enumerate any additional elements that may be required (and in what context). This would eliminate uncertainty about what constitutes a sufficiently complete DPIA.

Comment 3 – Redundancy should not create repetitive questioning (p. 4)

Cited text: "Certain **redundancy** between the DPIA template sections ensures that each mandatory element is addressed explicitly and in a traceable manner, while enabling cross-referencing. Furthermore, the same fact serves different functions across sections."

MDT view: Some level of redundancy is conceptually useful, because certain information may need to be considered under different angles: description of the processing, necessity, proportionality, risks, safeguards and residual risks. However, in operational practice, repeated questions may create frustration for business teams, such as clinical teams, IT teams or other

contributors, especially where they are asked to provide the same information several times. This creates the GDPR exhaustion and aversion complicating the work of privacy teams.

Suggested improvement: The text should encourage controllers to reuse information already collected, rely on cross-references where appropriate, and engage business or operational teams only where new information, confirmation or clarification is genuinely required. This would preserve the traceability objective while making the DPIA process more proportionate and workable.

Comment 4 – Lack of distinction between mandatory and optional elements (p. 4)

Cited text: "... DPIA template sections ensures that **each mandatory element** is addressed explicitly and in a traceable manner, while enabling cross-referencing."

MDT view: While the explainer acknowledges mandatory elements exist, it does not clearly distinguish them from optional or recommended elements throughout the template. This lack of differentiation creates confusion for practitioners and risks inconsistent application across organisations and jurisdictions. From our perspective, a detailed data flow description and a comprehensive asset inventory are non-negotiable must-have elements of any DPIA, regardless of its scope or trigger. The graphical or schematic data flow are "welcome" in the template, which is not appropriate in our view. Verbatim description of the data flow does not enable to properly assess the risks and safeguards in place for different segments of the data flow. The generic statement of "state of the art encryption is in place" for example is acceptable for a contract, but not for a DPIA, which shall confirm that encryption standards, potentially different segment by segment, are indeed all acceptable in the view of the context.

An important distinction that the current explainer does not address is the difference between two fundamentally different DPIA scenarios:

- **DPIA mandated by GDPR or national law** (e.g. Article 35(3) GDPR, national blacklists, sector-specific requirements): in these cases, the full template should be treated as mandatory insofar as each section is applicable to the specific processing activity. Controllers should not be able to selectively omit sections without documented justification, and supervisory authorities should be able to rely on a complete, consistent record.
- **Voluntary DPIA** conducted by a controller who has not met a formal trigger but considers the exercise necessary or beneficial (e.g. as a matter of good practice, risk management, or internal governance): in these cases, controllers may reasonably wish to adopt a proportionate, scoped approach — a so-called "light DPIA" — focusing on the elements most relevant to the processing activity at hand. The guidance should explicitly acknowledge this possibility and provide clarity on what a light DPIA may legitimately omit, rather than leaving controllers uncertain about whether a partial assessment is at all acceptable under some circumstances.

In both scenarios, however, the data flow description and the asset inventory must remain mandatory. These two elements are the analytical backbone of any meaningful DPIA: without a

documented data flow, it is impossible to properly identify risks, assess necessity and proportionality, or evaluate the effectiveness of security measures; without an asset inventory, the risk assessment lacks the technical grounding needed to be credible. If only two elements of the template were to survive in any version of a DPIA, mandatory or light, it is these.

Suggested improvement: Each field or section of the template should be explicitly labelled as either **mandatory** (M), **recommended** (R), or **contextual** (C), anchored to specific GDPR provisions where applicable. The guidance should introduce a clear two-tier framework distinguishing between full DPIAs required under GDPR or national criteria and light DPIAs conducted voluntarily, with explicit guidance on what may be scoped out in the latter case. In both tiers, the data flow description (section 1.2) and the asset inventory (section 1.3) should be unambiguously designated as mandatory, with the explainer stating clearly that a DPIA lacking either of these elements will be considered incomplete regardless of the trigger for the assessment.

Comment 5 – Duplication with Joint Controller agreements (section 0.1)

Cited text: "If applicable, identify Joint controllers. Clearly **define each party's obligations and tasks.**"

MDT view: Requiring a full definition of each joint controller's obligations and tasks within the DPIA creates unnecessary duplication with the joint controller arrangement required under Article 26 GDPR. Maintaining two parallel documents with the same information introduces inconsistency risk and administrative burden.

Suggested improvement: The template should require only identification of joint controllers, with a cross-reference to the Article 26 arrangement. The suggested wording could be: "*If applicable, identify joint controllers and refer to the applicable joint controller arrangement (Article 26 GDPR) for the definition of each party's obligations and tasks.*"

Comment 6 – Exhaustive listing of sub-processors within the DPIA is not always operationally feasible (section 0.2 & 1.2)

Cited text: "Identify the processors/**sub-processors** involved in the processing with the unequivocal definition of their obligations and tasks." And "Include information about the full chain composed of controller, processors **and sub-processors.**"

MDT view: In practice, it is not always possible for a controller to exhaustively list all sub-processors within a single DPIA document at the time of its completion. This is particularly acute where processors are large, globally operating organisations that dynamically allocate processing tasks across different entities, subsidiaries, or geographic locations within their group, with different organisational units potentially intervening at different points in time throughout the lifecycle of the processing.

Article 28 GDPR explicitly contemplates that controller authorisation for sub-processors can be **general** rather than specific. The Commission's standard contractual clauses operationalise this

through a list-based mechanism: the controller pre-approves a list of sub-processors, and the processor notifies any changes in advance (possibly by email), giving the controller the opportunity to object.

This model is legally sufficient under GDPR. It demonstrates that the controller maintains meaningful oversight of the sub-processor chain without requiring exhaustive real-time enumeration of every sub-processor in every document, including the DPIA.

Requiring the DPIA to list all sub-processors exhaustively would therefore go beyond what GDPR itself demands, create an artificial duplication of the contractual sub-processor list, and produce a DPIA that is either instantly outdated or requires continuous revision every time the processor updates its sub-processor list. The contractual mechanism under Article 28 and the SCC is precisely designed to manage sub-processor changes dynamically; DPIA should reference that mechanism, not attempt to replicate it.

A more operationally sound and legally coherent approach is using the provision of the Art. 28.3.f of GDPR requiring each processor to conduct a part of DPIA or a scoped assessment covering its segment of the processing, including the identification of its sub-processors. The controller would then collect either the full processor-level DPIAs or their documented conclusions and incorporate these by reference into the overarching controller-level DPIA. This model preserves accountability at each level of the processing chain, reflects the reality of complex multi-party processing arrangements, and avoids placing an unrealistic documentation burden on the controller alone. This approach should be explicitly recognized in the EDPB guidance as a valid means of meeting the DPIA requirement in complex processing chains.

Suggested improvement: The template and explainer should explicitly acknowledge that exhaustive listing of all sub-processors within a single controller-level DPIA is not always operationally feasible and should not be required as an absolute condition. The guidance should recognise cascaded DPIA delegation as a valid compliance model, whereby processors are required by contract to conduct their own scoped assessments covering their sub-processors, and controllers collect and reference these assessments or their conclusions. This is particularly relevant and should be explicitly addressed for processing activities involving global processors with dynamic internal task allocation. The template should provide a field allowing controllers to document this delegation arrangement and reference the collected processor-level assessments, rather than requiring direct enumeration of all sub-processors in the controller's own DPIA. On the other hand, this template is an opportunity to clarify that, part of compliance with the Art. 28.3.f, processors must transparently share the data flows and the list of assets supporting this data flow relevant to the activities performed on behalf of the data controller, including information necessary to map all eventual transfers of data outside of EU.

Comment 7 – Duplication with processor agreements (section 0.2)

Cited text: "Identify the processors/sub-processors involved in the processing with the unequivocal definition of their obligations and tasks."

MDT view: The obligations and tasks of processors and sub-processors are already governed by Data Processing Agreements under Article 28 GDPR. Reproducing this information in the DPIA is redundant and creates a risk of divergence between documents.

Suggested improvement: The template should require identification of processors and sub-processors (within the limits of our prior comment) and a reference to the relevant DPA, rather than a full restatement of obligations. Suggested wording: *"Identify processors and known to the date sub-processors involved. Refer to the applicable Article 28 GDPR agreement for the definition of their obligations and tasks."*

Comment 8 – End date requirement not applicable to ongoing processing (section 0.4)

Cited text: "Provide the estimated end date or expiration conditions (if applicable, i.e. because the processing is temporary, for example, associated with a project with a limited duration)."

MDT view: While the template acknowledges this field is conditional, many core organisational processing activities are ongoing with no foreseeable end date. The current framing may create pressure on controllers to artificially define end dates where none exist or leave a prominent field blank without clear guidance.

Suggested improvement: The template should include an explicit option such as *"Ongoing / no pre-defined end date"* as a valid response, with guidance that this is expected and acceptable for routine business processing activities.

Comment 9 – RACI matrix placement and governance references (section 0.5)

Cited text: "Identify the team involved in conducting this DPIA. You can provide details of their roles, tasks, responsibilities, etc. A **RACI** (Responsible, Accountable, Consulted, Informed) matrix can be used."

MDT view: For organisations with mature governance structures, RACI matrices are maintained in standard operating procedures or governance frameworks applicable across all DPIAs. Requiring or suggesting a RACI in each individual DPIA creates unnecessary duplication and administrative overhead.

Suggested improvement: The template should allow controllers to either include team information directly or reference an existing governance document. At minimum, the field should require the names and roles of individuals directly involved in producing this specific DPIA, with a cross-reference permitted to the applicable SOP for broader RACI governance. The text can be amended to: "Identify the team *directly* involved in conducting this DPIA. You can provide details of their roles, tasks, responsibilities, etc. A **RACI** (Responsible, Accountable, Consulted, Informed) matrix can be used, *unless clearly stated in the internal standards and procedures referred to within DPIA; in this case simply refer to it.*"

Comment 10 – DPO recommendation as a trigger for DPIA (section 0.5)

Cited text: "Explain the reasons to conduct the DPIA. It may be mandatory or there may be reasons that, in the opinion of the controller, make the DPIA necessary or beneficial."

MDT view: The explainer omits an important scenario: a DPIA conducted following a recommendation by the Data Protection Officer. Under Article 39(1)(c) GDPR, the DPO has a specific role in advising on DPIAs. A DPO recommendation to conduct a DPIA is a distinct and legitimate trigger that should be explicitly acknowledged. Last, but not the least the one can expect more mature organisations having an internal standard that required a DPIA. This option can also be added by default.

Suggested improvement: Add "DPO recommendation" and "Internal standard" as an explicit checkbox options in the list of reasons to conduct a DPIA, alongside mandatory triggers and controller-initiated assessments.

Comment 11– Formal approval is appropriate but should remain governance-based (section 0.5)

Cited text: "The DPIA must be formally approved by a responsible official (Managing Director, CEO, etc.) as complete and finished. The DPIA template might include a seal and signature."

MDT view: This is a positive requirement. A DPIA should not remain a purely legal or technical document; it should lead to a documented executive decision. Formal approval also supports accountability and makes it clearer who accepts the residual risk or eventually decides that the processing should not proceed. However, requiring CEO or Managing Director sign-off on every DPIA is disproportionate and operationally unworkable for large organisations processing significant volumes of data. DPIAs are frequently highly technical documents that senior executives are not well-positioned to evaluate, and this requirement risks becoming a rubber-stamping formality or creating bottlenecks.

Suggested improvement: This requirement should be kept and further emphasised but clarified to reflect that the "responsible official" should be determined according to the controller's governance model and the nature of the processing. Approval may appropriately come from a Head of Department, processing activity owner, project sponsor, risk committee or another accountable decision-maker provided the governance and RACI are documented in a policy, charter or any other relevant document and are in general aligned on the overall governance and responsibility allocation of the organisation. Suggested wording: "The DPIA must be formally approved by an accountable responsible official at an appropriate governance level, as determined by the controller's internal governance framework."

Comment 12 – Secondary use compatibility assessment (section 1.1.3)

Cited text: "Refer to an existing analysis (documented somewhere, not in this template) or examine any secondary or compatible uses of the data. State clearly whether data listed in 1.1.1

may be re-used for another purpose, and under what conditions, applying the purpose limitation principle."

MDT view: The current framing points to several distinct scenarios that warrant different treatment. A secondary use is, by definition, a separate processing activity; attempting to document all potential secondary uses within a single primary DPIA is neither practical nor conceptually appropriate. The relationship between primary and secondary processing activities should instead be managed through a clear linking mechanism, but this does not need to sit within the DPIA itself; the records of processing activities or equivalent governance documentation are a more natural home for this.

The guidance should distinguish between at least three scenarios:

Scenario 1 - Secondary use is itself subject to a mandatory or voluntary DPIA. In this case, the secondary use warrants its own standalone DPIA, which should include the compatibility assessment as an integral part. It is sufficient for the primary DPIA to acknowledge that secondary uses exist or are contemplated and to cross-reference the relevant child DPIA.

Scenario 2 - Secondary use does not trigger a DPIA. In this case, a standalone compatibility assessment should be conducted and documented separately, outside the primary DPIA. Again, the primary DPIA need only acknowledge the existence of the secondary use and reference the relevant compatibility documentation.

Scenario 3 - No secondary use is currently contemplated. The controller should state this explicitly and commit to revisiting the question, updating the relevant documentation, whether the DPIA or the records of processing activities, if secondary uses arise in the future.

In all scenarios, what matters is that a clear and navigable link is maintained between the primary processing activity and any secondary uses, so that the full picture of data use can be traced. However, this linkage function can and should be performed within the records of processing activities rather than loading the primary DPIA with information about activities that are analytically separate from it. On the other hand, for the scenario one, the template can state that if DPIA is conducted for the secondary use, the compatibility test (when applicable) shall be a part of it.

Suggested improvement: The section should be restructured to reflect the above scenarios explicitly, making clear that secondary uses are separate processing activities requiring their own documentation and, where applicable, their own DPIA which shall indeed include the compatibility test, unless not applicable. The primary DPIA should require only an acknowledgement of known or contemplated secondary uses and a cross-reference to the document containing relevant child documentation. The guidance should clarify that the linkage between parent and child activities can be maintained within the records of processing activities or equivalent governance records, rather than within the DPIA itself.

Comment 13 – Data flow as a mandatory element (sections 1.2 and 1.3)

Cited text: " Explain the data lifecycle and data flows: provide a comprehensive overview of how personal data is managed throughout its entire lifecycle, from collection to deletion."; on the template: "Note: Ideally, this table should be supplemented with one or more diagrams representing data flows or a similar figure."

MDT view: We strongly welcome the inclusion of graphical /schematic data flow documentation in the template. A comprehensive data flow description is foundational to any meaningful DPIA; without it, it is impossible to properly identify risks, assess necessity and proportionality, or evaluate the impact of security measures. Data flows must be treated as a mandatory, not optional ("ideally"), element of the DPIA.

Suggested improvement: Section 1.2 should be explicitly designated as **mandatory**. The explainer should state unambiguously that a DPIA lacking a documented data flow will be considered incomplete. On the other hand, verbatim description shall be optional. The template could further provide a minimum structure for the data flow description, covering: all involved stakeholders, systems, countries of where data are stored, transitioning through or consulted from, meaningful for the context indication of categories of data (for example being able to distinguish flows of normal only vs sensitive data containing flows or fully identifiable vs pseudonymous flow segments), indication of the way data transit from one stakeholder to another or from one system to another.

Comment 14 – Data quality metrics are insufficiently explained (section 2.2.2)

Cited text: "Provide data quality metrics, requirements or thresholds."

MDT view: This requirement is notably brief and, for many practitioners, will be unfamiliar territory within the context of a DPIA. Data quality as a GDPR principle under Article 5(1)(d) is well established, but the translation of this principle into concrete "metrics, requirements or thresholds" as documentation within a DPIA is a new and unexplained expectation. The current single-sentence instruction provides no indication of what level of detail is expected, what form metrics should take, or how they relate to the risk assessment and compliance analysis in other sections of the template.

In practice, data quality requirements vary significantly depending on the nature of the processing. A clinical trial dataset has entirely different accuracy and completeness requirements compared to a marketing database or an HR system. Without examples or a minimum structure, controllers will interpret this requirement inconsistently, and supervisory authorities will apply it inconsistently, undermining the harmonisation objective the template is designed to serve.

Suggested improvement: The EDPB should provide concrete examples of what data quality metrics, requirements or thresholds may look like across different processing contexts. At minimum, the explainer should clarify:

- what types of measures or indicators are expected (e.g. accuracy checks, completeness rates, validation rules, data refresh frequencies, source reliability assessments);
- whether quantitative thresholds are required or whether qualitative descriptions are acceptable;
- how this section connects to the necessity and proportionality analysis in section 3 and the risk assessment in section 4;
- how controllers operating in regulated sectors, such as clinical research, where data quality requirements are already governed by GCP, ICH E6 or equivalent standards, may cross-reference existing quality frameworks rather than duplicating them within the DPIA.

Without such clarification, this requirement risks becoming either a meaningless formality or an unexpectedly burdensome obligation, neither of which serves the purpose of meaningful data protection accountability.

Comment 15 – Transitional provisions

Cited text: None (no transitional provisions)

MDT view: Compliance with this template requires some serious investment. Some data controllers may realise that DPIAs they've conducted are not compliant with the new requirements. Publicly available DPIA registers from some large hospital organisations illustrate the operational scale of DPIA governance in healthcare. Some hospital registers include DPIA reference numbers exceeding 200 or even more, showing that large hospitals may need to maintain, update and review a high volume of DPIAs across areas such as clinical systems, research, digital tools, patient communications, imaging, occupational health, cybersecurity and service improvement initiatives. The same would apply to other health sector stakeholders, such as clinical trial sponsors, frequently performing a DPIA per clinical trial, since none of them is alike. We suggest leaving data controllers with 2 years from the date of publication of the final documents to update the DPIAs of processing activities that are still ongoing.

Suggested improvement: Adding a section on transition arrangements. Suggested wording:

“The EDPB acknowledges that compliance with this template represents a significant operational undertaking for many controllers, particularly those operating in sectors characterised by high volumes of processing activities subject to DPIA requirements, such as healthcare, clinical research, and pharmaceutical development.

For these and similarly positioned controllers, bringing all existing DPIAs into conformity with the requirements of this template in a short timeframe would not be operationally feasible without diverting significant resources from other data protection priorities.

*In recognition of this operational reality, controllers are given a transitional period of **two years from the date of publication of the final version of this template** to update DPIAs covering processing activities that are still ongoing at that date. During this transitional period, existing DPIAs that were conducted in good faith under previously applicable guidance or established*

methodologies shall continue to be considered valid documentation of compliance with Article 35 GDPR, provided they remain accurate and up to date in substance.”

Comment 16 – Full enumeration of processing operations should be supported (Type of operations, section 1.x)

Cited text: "Type of operations" / "Processing phase or stage".

MDT view: To be complete against the definition of "processing" in Article 4(2) GDPR, the template should ensure that the full range of processing operations can be recorded for each phase or stage. Leaving the field open invites under-inclusive answers and inconsistent completion, which weakens both the description of the processing and the downstream risk and necessity analysis that depend on it.

Suggested improvement: The template should provide the complete set of operations defined in Article 4(2) GDPR as selectable items, namely: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Providing these as a checklist (with the ability to add free text where needed) would guarantee coverage of every operation type in alignment with GDPR art 4(2) and improve comparability across DPIAs.

Comment 17 – Risk assessment should weight high-exposure processors (Risk Assessment and Management)

Cited text: "Risk Assessment and Management" (identification of processors within the risk analysis).

MDT view: The risk methodology does not appear to distinguish the processors that contribute most significantly to risk from those that do not. In practice, the processors that matter most are the main processors, those with ongoing or persistent access to the data, and those processing special categories of data under Article 9 GDPR. Treating all processors uniformly understates the exposure that these high-impact actors create and produces a risk picture that does not reflect operational reality.

Suggested improvement: The template should allow controllers to flag and weight high-exposure processors within the risk assessment, distinguishing at least: main processors; processors with ongoing or persistent access; and processors handling special-category or otherwise sensitive data. This ensures the analysis reflects the elevated contribution of these actors to the risk to data subjects, consistent with Articles 32 and 35(7)(c) GDPR.

Comment 18 – Risk methodology and risk metrics need proportionate guidance, especially for new processing (Risk method / Risk metrics)

Cited text: "Explain the details of the method followed to assess and manage risk and provide the necessary information to interpret the following: likelihood and severity levels and their

meanings (often a 2 to 5 levels scale is used); risk metrics; how to prioritise risks; risk acceptance levels. If an established method is used, provide the link to the external source introducing this method."

MDT view: Leaving the methodology entirely open is appropriate for mature organisations that already operate an established risk method, but it is less helpful for less mature controllers, who generally expect guidance and a stated rationale for the chosen scale and thresholds. A related difficulty arises with quantified risk metrics: requiring a risk score is demanding for a new or not-yet-operational processing activity, where the empirical data needed to derive a score does not yet exist. Without guidance, controllers are left uncertain whether reasoned assumptions are permitted as a basis for scoring.

Two clarifications would materially improve workability:

- For new or not-yet-operational processing, the explainer should confirm that controllers may base risk scoring on reasonable, documented assumptions, and should give guidance on how to state and justify those assumptions transparently so that the score remains auditable and can be revisited once the processing is live.
- The guidance should retain the flexibility to reference an established external method (with a link), while offering light-touch default guidance, for example an illustrative two-to-five-level likelihood and severity scale and example acceptance thresholds; so that less mature controllers have a defensible starting point and more mature controllers remain free to substitute their own method.

Suggested improvement: The explainer should (i) expressly permit assumption-based risk scoring for new processing, with a requirement to document and justify the assumptions; and (ii) provide an optional default scoring framework (illustrative likelihood/severity scale, prioritisation approach and acceptance levels) that controllers may adopt or replace with an established methodology referenced by link; last but not the list (iii) emphasize the importance of a thorough and exhaustive maintenance of the history of the data breaches, including those with no risks to the rights and freedoms of data subjects or even incidents where risk did not materialized as this is what the risk metrics are deriving from (among other sources).

Comment 19 – Technical measures are under-represented, and the residual-risk conclusion lacks a quantification mechanism (Technical and organisational measures)

Cited text: "Technical [and organisational measures supporting security of processing] - Implemented".

MDT view: Technical measures appear under-represented relative to organisational measures, and the template provides no mechanism to quantify or justify the resulting risk score. Without a way to demonstrate how technical controls reduce the likelihood and severity of risks, the residual-risk conclusion tends to be asserted rather than evidenced. This weakens the evidential link between the security measures recorded under Article 32 GDPR and the residual-risk determination that Article 35(7)(c) and (d) require, and it makes the analysis harder for supervisory authorities to follow.

Suggested improvement: The template should strengthen the technical-measures section and add, or reference, a quantitative risk-scoring mechanism (a risk calculator or equivalent) that lets controllers show how specific technical and organisational measures reduce likelihood and severity, so that the residual-risk conclusion is justified rather than asserted. Where a controller already operates such a mechanism within its chosen methodology, a cross-reference to it should be sufficient. It would be also useful to provide a sort of a check-list for a minimal types of technical measures to be systematically checked (segment by segment of the data flow); such as access control, encryption and key management, pseudonymisation (e.g. coding, tokenisation, keyed/salted hashing), logging monitoring and traceability, integrity and accuracy controls, backup resilience and recovery, retention and secure deletion, transfer and boundary controls, segregation and isolation, rights-enabling capabilities (ability to retrieve, export, rectify, restrict, delete data, and suppress automated decisioning)

Conclusion

We appreciate the EDPB's effort to harmonise DPIA documentation across the EU. The template provides a useful framework, but its practical utility would be significantly enhanced by clearer mandatory/optional distinctions, reduced duplication with existing legal instruments, explicit recognition of operational realities such as ongoing processing and DPO-triggered assessments, scalable approval governance, and practical prompts to support non-legal stakeholders in completing the more substantive analytical sections. We stand ready to engage further with the EDPB in refining this instrument.