Please, note that *this response is submitted by an independent practitioner with experience in data protection compliance and privacy risk assessment for large-scale digital processing environments.*

Public Consultation Submission: EDPB DPIA Template

A clear understanding of data flows is fundamental to conducting a meaningful assessment of privacy risks, particularly in the context of large-scale or complex processing activities. This is consistent with the accountability principle in Article 5(2) GDPR, the controller's responsibility under Article 24 GDPR, and Article 35(7) GDPR, which requires a systematic description of the processing as part of a DPIA. Recital 84 further emphasises the need to assess the likelihood and severity of risks to individuals' rights and freedoms. The EDPB's own Guidelines on DPIAs (WP248) reinforce this, recognising that a thorough description of processing operations — including data flows, system architecture and data recipients — is a prerequisite for identifying and assessing those risks.

At the same time, accountability expectations should be proportionate to the nature, scale and complexity of processing. Not all organisations can be held to the same standards, and the appropriate depth of data mapping should reflect that reality. For SMEs and organisations whose core business is not digital services, manual or simplified approaches may be entirely adequate, provided they give the organisation a genuine understanding of its processing activities and associated risks in line with GDPR accountability requirements. For these organisations, the template may serve primarily as guidance rather than a prescriptive step-by-step process.

For organisations running large-scale or highly automated processing environments, the picture is different. In these contexts, risks, mitigations and residual risks cannot be properly assessed without a comprehensive understanding of the end-to-end data lifecycle. This is where visual data flow mapping becomes essential — and where the current template, in sections 1.2 and 1.3, could go further.
A diagram representation of the data journey, from the point of collection through processing, storage, transfer and onward use, until data is returned to the individual as part of a product or service, makes it possible to identify precisely where technical and organisational safeguards are applied and whether they are applied at the right points. A list of measures, however detailed, cannot substitute for this level of visibility. To illustrate this in practice:

> A health platform may apply encryption at the point of data collection, but if data is subsequently passed to an analytics pipeline in unencrypted form before being aggregated and returned to users as personalised health insights, the safeguard does not cover the stage of the journey where the risk is actually highest. A financial services provider may document access controls at system level, but those controls may not follow the data when it is replicated to backup environments or shared with third-party scoring models. A large digital platform may have a defined retention

period at the application layer, while copies of the same data persist in logging systems or downstream vendor environments, rendering the retention policy ineffective in practice.

In each case, the measure exists on paper but does not hold across the full data journey — and this gap will not surface without a mapped, visual view of that journey. This matters particularly at what might be called the *return-as-a-service* moment — when raw or processed data comes back to the individual as a recommendation, a credit score, a personalised feed or an automated decision. This is frequently where the most sensitive inferences are drawn and where the cumulative effect of earlier processing becomes visible, however rarely mapped explicitly in DPIAs.

From this perspective, information relating to data categories, processing locations, system architecture, data recipients, transfers and access should not be viewed primarily as a compliance burden. Rather, establishing an operational mechanism — for example, integrated data mapping tools linking each DPIA entry to its corresponding ROPA entry and vice versa — should be seen as a core accountability exercise that strengthens the controller's ability to demonstrate verifiable compliance. For large digital platforms and services, this operational linkage, supported by visual data flow mapping, should be considered a core accountability mechanism rather than supplementary documentation.

The question should not be whether such information exists, but how it can be efficiently maintained and leveraged across accountability artefacts. In practice, much of this information already exists within large organisations for purposes such as security, incident response and vendor management.

A proper operationalisation of the DPIA also makes available a category of information that supervisory authorities regularly seek in the course of investigations and audits but which the current template makes no provision for — for example, timestamps and control versions. When a processing activity changes, when a safeguard is updated, when a new recipient is added or a transfer mechanism is amended, the ability to record precisely when that change occurred and which version of a control was in place at any given point in time is essential for demonstrating compliance historically, not only at the moment of assessment. This information is particularly difficult to maintain manually in fast-paced or complex digital environments, where processing configurations can change frequently and at scale. A well-operationalised DPIA framework, linked to live ROPA entries and supported by automated version tracking, would make this governance information systematically available — strengthening both internal accountability and the organisation's ability to respond to regulatory scrutiny in a meaningful and evidenced way.

The operationalisation of DPIAs in the context of AI systems raises a further and distinct challenge that the current template may not fully address. Article 35(3)(a) GDPR specifically contemplates situations involving a systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing — precisely the context in which AI systems operate. Yet a DPIA conducted at the point of system design or initial deployment captures the risk profile of the processing as it exists at that

moment only. In AI contexts, the risk to data subjects does not remain static. Models evolve, outputs change, inferences compound over time, and the cumulative effect of processing on individuals' rights and freedoms may look quite different months after a system goes live than it did at the point of the original assessment. The data collected at intake is only the starting point — what the system does with it, and what it produces as an output over time, is where the privacy impact is often most significant and least predictable. Therefore, the template must explicitly accommodate an iterative, lifecycle-based approach to DPIAs rather than a single, static pre-deployment assessment—the maturity of how these assessments are operationalised serving as a direct indicator of compliance with accountability provisions under the GDPR.

WP248 already acknowledges that DPIAs should be reviewed when the processing changes, but this has never been operationalised in a way that reflects the reality of AI systems operating at scale. For large-scale or complex AI-driven processing, a one-time DPIA is insufficient. What is required is a continuous or iterative assessment process — one that tracks not only changes to data inputs but the evolution of model outputs, the emergence of new risk vectors, and the changing impact on data subjects over the lifecycle of the system. This is particularly relevant where processing involves profiling, automated decision-making or systems that adapt based on user behaviour, all of which can materially alter the risk profile of the processing without any change to the underlying data collection.
This challenge is further compounded by the pace of digital technologies. At large scale and for complex data processing environments, the manual effort required to maintain and update DPIAs in line with these changes is practically unsustainable. Relying on manual processes alone makes it difficult for organisations to ensure meaningful accountability at the pace at which systems evolve — and creates a structural gap between the compliance framework and operational reality. This is not a reason to lower accountability expectations, but it is a reason for the Guidelines to acknowledge that for large-scale AI-driven processing, automated or semi-automated DPIA review mechanisms may be necessary to maintain genuine rather than nominal compliance, with all updates linked to the corresponding ROPA entries to preserve a coherent and auditable accountability record.
It is also worth noting that the AI Act now imposes its own risk assessment obligations for high-risk AI systems, many of which will simultaneously require a DPIA under GDPR. The current template does not address this intersection. Ensuring operational coherence between GDPR accountability requirements and AI Act obligations.

Suggested clarification on 3 points

---

1. For large-scale or high-risk processing, visual representations of the end-to-end data journey should be explicitly encouraged within sections 1.2 and 1.3 of the template, that documented traceability across accountability artefacts should be recognised as a core requirement consistent

with Article 24 GDPR, and that each DPIA entry should where possible be linked to the corresponding ROPA entries to ensure coherence across accountability documents.

2. For for AI-driven processing falling within the scope of Article 35(3)(a) GDPR, the DPIA should be understood as a living document subject to continuous review, with the template providing explicit guidance on how to document and trigger iterative reassessments as outputs evolve and risk profiles change, including provision for timestamping changes and versioning controls so that the state of compliance at any given point in time can be reconstructed and demonstrated to supervisory authorities.
3. Guidelines should acknowledge the intersection with AI Act obligations and encourage an integrated approach to risk assessment that avoids unnecessary duplication while ensuring that both frameworks are satisfied in substance.