The Illusion of Assurance: A Critique of the 2026 EDPB DPIA Template

The European Data Protection Board's release of the 2026 Data Protection Impact Assessment (DPIA) template represents an ongoing effort to standardize privacy compliance across the industry. The template's structured fields are a welcome step toward traceability. However, for privacy engineers and data scientists, a critical review reveals a significant gap between bureaucratic compliance and mathematically defensible data protection. Instead of elevating privacy to a rigorous engineering discipline, the template perpetuates a system heavily reliant on subjective, qualitative risk assessment.

The Missing Link: PII, Linkability, and Quantification

Perhaps the most glaring omission is the complete lack of quantitative frameworks for defining data sensitivity. International standards like ISO 29100 and ISO 29134 are built around Personally Identifiable Information (PII) and the specific degree to which data is linkable.

To be legally precise, the GDPR uses "personal data" rather than "PII," as the European definition is broader. The template reflects this by asking assessors to list "Processed personal data" in Section 1.1.a. However, this legal distinction does not excuse the engineering shortcoming of the framework. The core characteristics of sensitive data—its semantic meaningfulness and exact degree of linkability—are completely ignored. There is no requirement, nor even a prompt, to quantify linkability or measure informational entropy. By failing to integrate these measurable dimensions, the template leaves data "sensitivity" assessment to subjective compliance judgments.

The Relegation of Rigorous Methodologies

Because the template relies on qualitative evaluations—with the Explainer suggesting "qualitative scales" for risk levels—rigorous lossy obfuscation techniques are relegated to cosmetic footnotes.

Advanced techniques like Differential Privacy (DP), Pointwise Maximal Leakage (PML), and Bayesian inference-based obfuscation fit into sub-sections:

- **Section 2.2.a (Data minimisation):** Technical constraints on utility.
- **Section 2.3.a (Article 5(1)(a-f)):** Data minimisation measures.
- **Section 2.3.d (By design/default):** System-level architectures.
- **Section 4.2.a (Mitigating measures):** Technical safety nets.

Yet each asks only for "discussion of appropriateness and effectiveness", not epsilon-DP bounds, leakage metrics, or proofs. Thus, state-of-the-art epsilon-DP equals basic masking on paper.

The Duty to Facilitate Verifiable Engineering

Template creators must enable rigorous assurance. DPIAs cannot remain narrative exercises if they are privacy's gold standard. Formal verification offers guarantees beyond risk matrices.

The EDPB should add fields for formal constructs like unlinkability (e.g., epsilon bounds, leakage values). These are quantifiable, auditable properties. By sidelining privacy science, the industry disincentivizes research, favoring fuzzy statements over verifiable engineering. Until templates demand quantitative methods, DPIAs remain compliance formality, not technical assurance.