Public Consultation Feedback: Future-Proofing the EDPB Common Template for AI-Enabled and Agentic Processing

Submitted in Response to Draft Version 1.0 (Adopted 08 June 2026)

While the draft template successfully standardizes data breach reporting across the EU, it suffers from an architectural gap regarding artificial intelligence, algorithmic inference, and autonomous agent systems. To ensure this framework remains resilient against the rapid emergence of agentic infrastructure, we propose the following precise modifications to the existing form fields, balancing forensic precision with data controller operational realities under the 72-hour notification constraint.

I. Granular Technical Modifications to Existing Fields

To avoid increasing administrative burdens or requiring a separate reporting framework, AI-specific risks can be seamlessly integrated into the template's existing dropdown options:

1. Expanding Section 3.2: Nature of the Incident (Field 60)

The current list in Field 60 is heavily optimized for traditional, static attack vectors (e.g., ransomware, phishing, CVE exploitation). It lacks the specific vocabulary required to identify modern algorithmic failure modes.

- **Recommendation:** Add the following predefined values to the **Field 60 Dropdown Options**:
    - *Exploitation of AI/LLM vulnerability (e.g., direct/indirect prompt injection, jailbreaking, model manipulation).*
    - *Autonomous system execution error / Unintended AI agent tool-call.*

2. Modifying Section 3.4: Type of Breached Data (Field 70)

Traditional data breach reporting assumes personal data is merely exfiltrated from a passive storage container (e.g., basic details, medical history). In AI environments, breaches frequently involve data that was never formally ingested but was dynamically inferred or reconstructed.

- **Recommendation:** Add a specific value to **Field 70**:
    - *Inference-generated or synthetic personal data (data dynamically derived or unmasked by automated systems rather than accessed from stored database tables).*

3. Modernizing Section 3.5: Technical and Organizational Measures (Field 75)

The existing template relies entirely on static, system-level safety proxies (e.g., encryption, periodic audits, policy documents). It fails to track whether an organization possesses dynamic, real-time control capabilities.

- **Recommendation:** Supplement the predefined options in **Field 75** with:

- *Runtime execution-layer guardrails / Dynamic authorization validation (verifying authority at the exact point of execution rather than relying on retrospective system-level credentials).*

II. Macro Operational and Cross-Border Considerations

Beyond static dropdown changes, agentic workflows present two systemic anomalies that the EDPB must address in the finalizing of this template:

1. Contextual Risk vs. Data Categories (Section 4.1 & 4.2)

The business logic of the form heavily links risk to the *volume and category* of personal data affected. However, when autonomous systems are involved, the risk to the data subject shifts drastically based on **contextual application** rather than the broad data category. Fully autonomous agent decisions require a heightened tracking of context-driven harm (such as automated financial or legal changes executed by an agent chain), which cannot be captured by a checkbox checking for "basic data".

2. Cross-Border Processing and Modular AI Chains (Section 6.2 & 6.3)

Modern agentic architectures are increasingly modular, routing parts of a single transaction across multiple external infrastructures on the fly (e.g., an EU orchestrator calling an external foundation model API or vector database).

Furthermore, shifting judicial realities and regulatory structures outside the EU demonstrate that institutional wrappers (such as foreign data privacy review bodies or third-country controllers) can dissolve rapidly. If an enterprise data processor utilizes third-party AI APIs or hosts model inference outside the EEA, a data leak occurring down that operational chain immediately disrupts standard Transfer Impact Assessments (TIAs). Sections 6.2 and 6.3 must explicitly ask controllers to declare whether an incident involved **automated, external third-party AI endpoints or cross-border modular inference pipelines** to effectively coordinate joint DPA responses.

Submitted by,

Sanjaya Gunasiri

Orchard Graphics
https://www.linkedin.com/in/sanjayagunasiri/