

Feedback on the EDPB DPIA Template: Tool-Assisted DPIA Preparation for Public-Facing AI Chatbot Processing

Submitter: Marius, individual contributor

Submission type: Public consultation feedback

Date: 2026-06-04

1. Introduction

I welcome the EDPB's draft DPIA Template and its objective of supporting more complete, consistent, and structured DPIA reporting across the EU.

This feedback is submitted from the perspective of an individual contributor working on tool-assisted DPIA preparation for public-facing AI chatbot processing. I am not asking the EDPB to validate any specific product, workflow, or chatbot deployment. The purpose of this submission is to provide practical feedback on how the DPIA Template could better support controllers who use software, AI assistants, document analysis, runtime testing, or similar tools when preparing DPIA materials.

The central point is simple: as DPIA preparation becomes more tool-assisted, the template should help controllers distinguish factual evidence, draft analysis, recommendations, human-reviewed findings, DPO advice, interested-party views, controller decisions, formal validation, and content intended for publication or external sharing.

This distinction is especially important for public-facing AI chatbots. Such systems may involve public notices, runtime behaviour, generated or inferred personal data, model/provider documentation, secondary-use questions, security controls, and data-subject rights issues. A tool may help collect and organize evidence, but it should not be confused with the controller's own legal assessment, risk acceptability decision, DPO advice, stakeholder consultation, prior-consultation decision, or formal sign-off.

2. Suggested Clarification: Tool-Assisted DPIA Preparation

The template could include an optional field asking whether the DPIA was prepared with the assistance of software, AI tools, automated document analysis, runtime testing, or similar tooling.

Where such tooling is used, the controller could briefly identify:

- what role the tool played;
- what source materials or observations it helped process;
- which outputs were human-reviewed;
- which sections remain controller-owned or human-owned decisions.

This clarification would be useful near the DPIA technical sheet, alongside information about the DPIA team, reference materials, scope, formal validation, and publication or sharing posture.

The aim is not to make tool use mandatory. The aim is to make tool-assisted preparation transparent where it occurs.

3. Suggested Clarification: Evidence, Draft Analysis, Recommendations, And Adopted Measures

The template could clarify how controllers should report proposed or recommended measures.

A proposed measure or recommendation should be clearly distinguished from:

- factual evidence;
- draft analysis;
- an implemented safeguard;
- a controller-approved mitigation;
- a final DPIA conclusion.

This distinction matters because tool-assisted or reviewer-assisted DPIA workflows may generate proposed actions before the controller decides whether to accept, reject, modify, or implement them. Without a clear distinction, a draft recommendation may be misread as an implemented measure or as a legal conclusion.

If the EDPB considers an action register or annex useful, it could record limited information such as:

- source of the proposed recommendation, for example DPO, human reviewer, external advisor, or tool-assisted draft;
- linked DPIA section, risk, or measure;
- controller disposition, for example accepted, rejected, modified, or pending;
- owner or responsible function, where appropriate.

This could sit outside the main template if the EDPB prefers to keep the template concise.

4. Suggested Clarification: Human-Owned Decisions

For fields involving legal adequacy, necessity, proportionality, risk acceptability, prior consultation, DPO advice, interested-party views, and formal validation, the template could explicitly signal that these are controller-owned or human-owned judgments, even when software helps gather evidence.

For example, evidence gathered from privacy notices, system documents, provider documents, runtime observations, or interviews may support the DPIA, but the evidence itself does not decide:

- whether the processing is legally adequate;
- whether necessity and proportionality are satisfied;
- whether residual risk is acceptable;
- whether prior consultation is required;
- what the DPO advises;
- what interested parties or data subjects consider important;
- whether the DPIA is formally validated.

Making this boundary explicit would reduce the risk that tool-generated summaries or evidence tables are mistaken for DPIA judgments.

5. Suggested Clarification: Publication And External Sharing For AI/Chatbot DPIAs

The template could clarify how controllers should handle publication or external sharing where the DPIA concerns AI/chatbot systems and contains security, model/provider, prompt, telemetry, or attack-surface

information.

The template already recognizes that publication may require care. For AI/chatbot systems, the line between useful transparency and security-risk disclosure may be difficult. Controllers would benefit from examples of what may be:

- published;
- summarized;
- withheld;
- referenced separately;
- retained only in internal evidence records.

This could be included near the publication or external-sharing part of the DPIA technical sheet.

6. Suggested Clarification: Evidence Traceability

The template could recommend that controllers maintain a traceable evidence register linking major DPIA statements to their supporting sources.

For AI/chatbot systems, evidence may come from many places:

- privacy notices;
- chatbot interface text;
- model/provider documentation;
- processor or recipient information;
- system architecture documentation;
- security documentation;
- runtime observations;
- transcripts or test interactions;
- interviews or controller-provided explanations.

The DPIA template itself should remain readable. A separate evidence register, annex, or reference list could help preserve traceability without overloading the main report.

7. Suggested Clarification: Generated Or Inferred Personal Data

For public-facing AI chatbot systems, the template or accompanying guidance could include examples on generated or inferred personal data.

Chatbots may generate, infer, summarize, classify, or transform information about individuals. Some outputs may be inaccurate. Some may imply sensitive attributes or other high-risk inferences. These issues may be relevant to:

- the description of processed personal data;
- the nature, scope, context, and purposes of processing;
- accuracy and data-quality assessment;
- data-subject rights;

- risk identification and mitigation.

The request is not for the template to resolve all AI-specific legal questions. Rather, practical examples would help controllers avoid overlooking generated or inferred personal data when preparing the DPIA.

8. Summary Of Recommendations

I recommend that the EDPB consider whether the DPIA Template or its explanatory materials should:

1. include an optional field for tool-assisted DPIA preparation;
2. distinguish factual evidence, draft analysis, recommendations, adopted measures, and final conclusions;
3. explicitly identify legal/risk/sign-off fields as controller-owned or human-owned judgments;
4. clarify publication and external-sharing boundaries for AI/chatbot DPIAs;
5. encourage traceable evidence registers or annexes;
6. provide examples for generated or inferred personal data in AI/chatbot processing.

These changes would make the template more useful for modern tool-assisted DPIA preparation while reinforcing that accountability, legal adequacy, risk judgment, stakeholder consultation, DPO advice, and formal validation remain with the controller and relevant human experts.