BEFORE YOU APPROVE

10 Questions Every DPO Should Ask

Before Approving an AI Tool for Regulated Workflows

A practical governance framework for Data Protection Officers at regulated EU firms.

PRESENTED BY

[Advisor / Organization Name]

[Title, Credentials, Contact]

Replace the three bracketed lines above with your name, credentials, and contact details; keep the rest unchanged. This guide is designed to be handed out at your seminar, included in your onboarding pack, or shared directly with clients under your brand.

How to Use This Guide

The DPOs who will be best positioned in the next 24 months are not the ones who blocked AI adoption. They are the ones who built the governance framework that made safe adoption possible.

Most organizations are already using AI tools informally. The goal of this guide is to formalize governance without slowing the business. Use it as a 20-minute approval checklist. Work through it before any new AI tool goes live in a regulated workflow. If any answer is "Not yet," capture the missing evidence, name an owner, and set a date. The scorecard at the end is designed to be used in a governance meeting.

This guide assumes GDPR fluency. It does not explain what a DPIA is or why Article 30 matters. It focuses on applying those concepts to the specific governance challenges created by AI tools, which most GDPR frameworks have not yet caught up with.

Part One: Legal Basis & Governance

1. Does this AI tool have a documented legal basis under GDPR?

Before any personal data enters an AI tool, you need a defensible legal basis. Legitimate interest requires a three-part test. Consent for AI processing is narrower than most organizations assume. Contract performance rarely extends to AI-assisted analytics. If the legal basis has not been explicitly mapped to this tool and this specific workflow, the processing is not compliant, regardless of what the vendor contract says.

> *Ask: Which Article 6 basis applies? Is it documented in your processing register? Has it been tested against this specific workflow, not just the tool category?*

2. Has a DPIA been completed, scoped, or formally deferred?

Article 35 DPIA requirements are triggered by systematic profiling, large-scale processing of sensitive data, or new technologies that present high risk. Most AI tools meet at least one criterion. A formal decision to defer a DPIA is not the same as having concluded one is unnecessary. If the answer is "we have not looked at it yet," that is your gap.

> *Ask: Who made the DPIA determination? Is it documented? If the tool processes EU data subjects' personal data at scale, DPIA criteria are often triggered. Document the determination either way.*

3. Who owns AI governance in this organization, and is that ownership documented?

AI governance accountability cannot be distributed by default across IT, Legal, and Compliance without a named owner per tool. The DPO's advisory role under GDPR includes AI tool selection. Advisory is not the same as ownership. If no one can say who is accountable when something goes wrong with this specific tool, that is a governance gap that will surface in an audit.

> *Ask: Is there a named governance owner for this tool? Is it documented in your data processing register? Does the DPO have a formal advisory role in the approval process?*

4. How does this tool interact with your existing data processing register?

Every new AI tool is a new data processing activity. Your Article 30 record of processing activities must reflect it: the tool, the purpose, the legal basis, data categories, flows, retention periods, and third-country transfers. If the tool cannot be fully mapped into your register, you do not have sufficient information to approve it.

> *Ask: Can you complete an Article 30 entry for this tool today? If not, what information is missing, and who is responsible for obtaining it?*

> ***If you can answer Q1 to Q4, you can defend approval decisions.***

Part Two: Data Flows & Risk

5. Where does personal data go when your team runs a query through this tool?

This is the question most DPOs have not fully answered for AI tools already in use. When a team member submits a query containing personal data, that data may leave your controlled boundary and be processed on vendor infrastructure. Depending on the tool, tier, and configuration, it may be retained, logged, used for model training, or accessible to vendor staff. A DPA is not a data flow map, and a privacy policy is not a DPA.

> *Ask the vendor directly: Where is data stored? In which jurisdiction? Who can access it? Is it used for model improvement? Ask for the answers in writing, such as a security whitepaper or DPA annex, not verbally. That converts the exercise into evidence you can produce.*

6. Can you demonstrate data minimization for this AI workflow?

Article 5(1)(c) requires that personal data processed is adequate, relevant, and limited to what is necessary. AI tools create a specific minimization risk: users often include more context than necessary in prompts because more context produces better outputs. That behavioral tendency, multiplied across a team, produces a systematic minimization failure. Both the tool design and the workflow design need to address this.

> *Ask: Has the workflow been designed to limit personal data in prompts to what is strictly necessary? Is there user guidance? Is it enforced by process or only by policy?*

7. What is your incident response plan for AI-generated content?

Hallucination in a regulated context is not merely a quality issue. If an AI tool generates a false adverse media finding, attributes an incorrect beneficial owner linkage, or fabricates a compliance-relevant conclusion, and that output is acted on or shared with a client, this may trigger an Article 33/34 breach notification scenario as well as professional liability. Most AI incident response plans do not yet address this category of output failure.

> *Ask: Does your incident response plan include AI-specific scenarios? Who triages AI-generated content that causes harm? Is there a verification step before AI outputs enter any deliverable or decision?*

> ***If you can answer Q5 to Q7, you can evidence control.***

Part Three: The Questions Most DPOs Have Not Asked Yet

8. Could you explain your AI data practices to a supervisory authority today?

This question is no longer hypothetical. Supervisory authorities across the EU are beginning AI-specific investigations. The organizations that can produce a clear, documented account of their AI tool inventory, legal bases, data flows, and governance decisions will be in a fundamentally different position. You do not need every answer. You do need to have asked every question and documented the process.

> *Ask: If your supervisory authority requested your AI governance documentation tomorrow, what could you produce? What would be missing? Who would need to be involved to fill the gaps?*

9. How do you handle data subject rights for AI-processed data?

When personal data is processed by an AI tool, data subject rights under Articles 15 to 22 still apply. The right of erasure is particularly complex: if personal data was used in a prompt that contributed to model outputs, what does erasure mean in that context? If personal data was retained by the vendor, does your erasure request reach it? These questions are not resolved by most vendor contracts.

> *Ask: Have you mapped how Articles 15 to 22 apply to this specific AI tool? What is the vendor's role as processor, separate controller, or joint controller for prompts, logs, and telemetry, and is that reflected in the DPA? Do you have contractual mechanisms to fulfill erasure and access requests for vendor-held data?*

10. Is your AI infrastructure designed for regulated data environments, or repurposed from something else?

Most AI tools were built for content creation, productivity, or general-purpose use. They were not designed for environments where the data is a high-risk individual, a sanctions-adjacent subject, a beneficial owner, or a patient whose health data is special category under Article 9. That design mismatch has compliance consequences. The right infrastructure for regulated workflows is one where personal data is designed to remain within your controlled boundary, not accessible to the vendor or any third party. That is an architecture question, not a policy question.

> *Ask: Is the confidentiality of data in this tool a function of architecture, or of vendor promises? Can you evidence the answer to a DPIA, a client questionnaire, or a supervisory authority?*

> ***If you can answer Q8 to Q10, you are inspection-ready.***

AI Governance Readiness Scorecard

Use this with your privacy advisor as a working governance artifact. If any item is Not Yet, name an Owner and set a Due date.

Question	Yes	Not Yet	Owner	Due
Legal basis for each AI tool in use is documented in the processing register	☐	☐		
A formal DPIA determination has been made and recorded for each in-scope tool	☐	☐		
AI governance ownership is named and documented for each tool	☐	☐		
Every active AI tool has an Article 30 entry including data flows and transfers	☐	☐		
A complete data flow map exists for each AI tool, including third-country transfers	☐	☐		
Workflows have been reviewed for data minimization compliance in AI prompts	☐	☐		
Incident response plan covers AI-specific output failures and hallucination scenarios	☐	☐		
AI governance documentation is ready to produce for a supervisory authority	☐	☐		
Data subject rights (Art. 15–22) have been mapped for each AI tool and vendor	☐	☐		
AI infrastructure was evaluated against regulated data environment requirements	☐	☐		

Mostly Yes	A Mix	Mostly Not Yet

Strong governance position. Work with your advisor to formalize your AI governance framework and prepare documentation for supervisory authority review.	Normal for most organizations. Use the Not Yet items as your preparation checklist before expanding AI adoption or responding to a supervisory inquiry.	Do not rush. Getting the foundations right first protects your clients, your organization, and your professional standing. This guide is your starting point.

Prepared for you by your privacy advisor.

Your advisor: _____

If the questions in Part Three resonated, ask your advisor about AI infrastructure designed for regulated workflows where personal data is designed to remain within your controlled boundary.

TOTALLY PRIVATE AI

Air-gapped AI for regulated environments.

totallyprivate.ai