Questions for [supplier] about [AI tool]

How to use: send this list to the supplier (or check their trust centre and data processing agreement first and only ask what is missing). The answers go into sections 2, 4 and 6 of your DPIA. Delete this box before sending.

Dear [contact],

We are assessing our use of [AI tool] for [purpose] under the GDPR (data protection impact assessment, Art 35) and the EU AI Act. Could you answer the questions below, or point us to the document where the answer is? Thank you.

Data use

1. **Training.** Do you use our inputs, files or outputs to train or improve any model? If there is an opt-out, how is it set and is it on by default for our plan?
2. **Roles.** Do you act as our processor (Art 28 GDPR) for this tool? Please send the data processing agreement that applies to our plan.
3. **Your own purposes.** Do you process our data for any purpose of your own (analytics, abuse monitoring, product improvement)? Which data, and for how long?
4. **Sub-processors.** Which sub-processors (including model providers) receive our data, and where are they?
5. **Location and transfers.** Where are inputs, outputs and logs stored and processed? For transfers outside the EEA, which safeguard applies (adequacy decision, standard contractual clauses)?
6. **Retention.** How long are prompts, files, outputs, recordings and logs kept? Can we set or shorten this, and can we delete them on request?

How the AI works

1. **Purpose and limits.** What is the tool designed and tested for, and what should it not be used for?
2. **Accuracy.** How do you measure accuracy and error rates for our kind of use? Known limitations?
3. **Bias.** How do you test for unfair results for groups of people (for example by sex, age, origin)?
4. **Human oversight.** Which features let our staff review, correct or override the output before it affects a person?
5. **Logs.** Which logs does the tool keep about its use and outputs, and can we export them?

Security

1. Certifications or reports (for example ISO/IEC 27001, SOC 2) that cover this tool.
2. Access control, encryption in transit and at rest, and how you notify us of a personal data breach (Art 33(2): without undue delay).

Sample — lerider.com

Sample — the full pack: lerider.com/shop/ai-dpia-check-eu/

EU AI Act

1. **Your role.** Are you the provider of this AI system under the AI Act? Who is the provider of the underlying model?
2. **Risk class.** Do you consider this system high-risk under Annex III for the use we describe? If you rely on the art 6(3) exception, can you share your assessment?
3. **Instructions for use.** If the system is high-risk, please send the instructions for use (art 13). We need them for our DPIA (art 26(9)).
4. **Transparency.** Does the tool tell people they are interacting with an AI system (art 50(1)), and does it mark generated content (art 50(2))?

Kind regards,

[Name, role, organisation]

Sample — lerider.com

Sample — the full pack: lerider.com/shop/ai-dpia-check-eu/

Data protection impact assessment: [AI tool or feature]

How to use: replace every [bracket]. Delete the guidance in italics boxes like this one when you are done. A DPIA must be done before the processing starts (Art 35(1) GDPR) and kept up to date. This template follows the minimum content of Art 35(7). It is a template, not legal advice.

Item	Fill in
Organisation (controller)	[Organisation name, address]
AI tool and supplier	[Tool, version or plan, supplier]
Workbook reference	[Ref from AI_Register]
DPIA owner	[Name, role]
DPO or privacy adviser	[Name, or: no DPO designated]
Version and date	[v0.1, date]
Review trigger	At least when the risk changes (Art 35(11)); our advice: yearly, and when the tool, the data, the purpose or the supplier changes

1. Why this DPIA

Screening result from the workbook: [DPIA required / DPIA likely needed (criteria: ...)]. Art 35(3) case: [yes, (a)/(b)/(c) / no]. On our supervisory authority's DPIA list: [yes, item ... / no].

2. Description of the processing (Art 35(7)(a))

Describe it so that someone outside the team understands it. For an AI tool, say what goes in, what the model does, what comes out and who acts on the output.

Question	Answer
Purpose: what do we use the AI for?	[...]
Lawful basis (Art 6) and, for special category data, the Art 9(2) condition	[...]
If legitimate interests: what is the interest?	[...]
Whose data (categories of people) and roughly how many?	[...]
Which personal data goes into the tool (prompts, files, recordings, records)?	[...]
What comes out (score, ranking, summary, text, decision) and who uses it?	[...]
Is a decision about a person made by the tool alone? (Art 22)	[yes / no; if yes, which Art 22(2) exception and which safeguards]
Does the supplier use our data to train or improve its models?	[yes / no / opt-out set on ...]
Where is data stored and processed? Transfers outside the EEA and safeguard	[...]
How long are inputs, outputs and logs kept, by us and by the supplier?	[...]
Processor agreement (Art 28) in place?	[yes, signed on ... / in progress]
Data flow: source, tool, output, storage, deletion	[short description or diagram reference]

Sample — the full pack: lerider.com/shop/ai-dpia-check-eu/

3. Necessity and proportionality (Art 35(7)(b))

Question	Answer
Why do we need AI for this purpose? What happens without it?	[...]
Could we reach the purpose with less data, or without data about people?	[...]
Data minimisation: what do we keep out of the tool? (instructions to staff)	[...]
Accuracy: how do we check the output before we rely on it?	[...]
Transparency: how and where do we tell people? (Art 13/14; AI Act art 50 where it applies)	[...]
People's rights: how do people get access, correction, objection, human review?	[...]

4. Risks to people (Art 35(7)(c))

Look at risks to the people whose data it is, not to the business. Rate likelihood and severity (low, medium, high) before measures. Typical AI risks are listed; delete what does not apply and add your own.

Risk	Likelihood	Severity	Why
Wrong or biased output leads to an unfair decision (e.g. an applicant rejected)	[ ]	[ ]	[...]
People do not know AI is used, or cannot get a human to review the outcome	[ ]	[ ]	[...]
Personal data in prompts or files is used by the supplier for training	[ ]	[ ]	[...]
Confidential or special category data is entered by staff without need	[ ]	[ ]	[...]
Output contains personal data that is wrong (hallucination) and is stored or shared	[ ]	[ ]	[...]
Monitoring of staff goes further than needed, chilling effect	[ ]	[ ]	[...]
Data breach at the supplier or in the integration	[ ]	[ ]	[...]
Data kept longer than needed in chat histories, logs or recordings	[ ]	[ ]	[...]
Transfer outside the EEA without a valid safeguard	[ ]	[ ]	[...]

Sample — the full pack: lerider.com/shop/ai-dpia-check-eu/