

Data protection impact assessment (DPIA) for an AI tool

Fill in the parts in square brackets. Keep the finished version with your project records and review it whenever anything changes. This template follows the ICO's seven steps. It isn't legal advice: your data protection officer or adviser makes the call.

Organisation	[Your business]
AI tool or project	[What it is, and the supplier]
Project owner	[Name, role]
Data protection officer or lead	[Name, role]
Started	[DD/MM/YYYY]
Version	[1.0]

1 Why you need a DPIA

What will the AI tool do, in one sentence?

Tick each that applies. Any tick is a reason to complete this DPIA:

- ☐ Personal data goes into the tool, or comes out of it
- ☐ It uses new technology, including AI
- ☐ It uses health, financial hardship or other sensitive data, or criminal offence data
- ☐ It helps make decisions about people that affect them significantly
- ☐ It monitors or tracks people
- ☐ It combines personal data from different sources
- ☐ It involves children or vulnerable people

2 Describe the processing

What goes in	[Prompts, documents, emails, recordings or files, and the personal data in them]
What comes out	[Drafts, summaries, answers or decisions, and who sees them]
Where it's processed and stored	[Country and service, including where support staff sit]
The supplier's role	[Processor acting on your instructions, or a controller in its own right]
What the supplier keeps	[Inputs and outputs kept, for how long, and whether they train its models]
Whose data, and how much	[Staff, customers or the public; roughly how many people; how often]
What people would expect	[Would they expect this use? Have concerns been raised before?]
The purpose	[What you want to achieve, and the benefit to you and to the people involved]

3 Consultation

Inside the business	[IT, security, the team who'll use it, and how you asked them]
The supplier	[What you asked for: terms, security information, data locations]
Your DPO	[When you asked for advice]
The people whose data it is	[How you asked them, or why you didn't]

4 Necessity and proportionality

Lawful basis	[Which basis applies, and why]
Less data	[Could you do this with less personal data, or none?]
Human checks	[Who checks an output before it's used about a person?]
Telling people	[Which privacy notice you'll update]
People's rights	[How you'll find and correct or delete their data in the tool]
The supplier contract	[Data processing terms in place, and their date]
Transfers	[Any processing outside the UK, and the safeguard used]

5 Risks to people

Risk to people	Likelihood Remote, possible or probable	Severity Minimal, significant or severe	Overall Low, medium or high
Personal data goes in that the tool didn't need			
Staff can see documents through the tool that they couldn't open before			
An inaccurate output about a person is used without being checked			
The supplier keeps inputs longer than expected, or uses them to train its models			
Data is processed or supported outside the UK without a safeguard			
Outputs treat some groups of people less fairly than others			
[Add your own]			

6 Measures to reduce the risks

Risk	Measure	Effect Eliminated, reduced or accepted	Remaining risk Low, medium or high	Approved Yes or no
[Risk from step 5]	[What you'll do]			
[Risk from step 5]	[What you'll do]			
[Risk from step 5]	[What you'll do]			

7 Sign off and record outcomes

Measures approved by	[Name, role, DD/MM/YYYY]
Remaining risks approved by	[Name, role, DD/MM/YYYY. If any high risk remains, consult the ICO before you start]
DPO advice given	[Yes or no, DD/MM/YYYY]
Summary of DPO advice	[What they advised]
DPO advice followed or overruled by	[Name. If overruled, say why]
Consultation responses reviewed by	[Name]
Kept under review by	[Name, and the next review date]