

AI DATA GOVERNANCE FOR LEADERS

“We pay for it, so our data is safe.” Usually wrong.

THE ASSUMPTION

WHAT IS ACTUALLY TRUE

1 *Paid plan means protected.*

Protection comes from a contract, not a price.
A DPA or commercial terms, not the tier name.

2 *Only the free plan is risky.*

Several paid personal plans can still train on
what you upload, unless you turn it off.

3 *Training is fixed by the plan.*

On most consumer tiers it is a setting you
control, not a property of the plan you bought.

4 *A SOC 2 or ISO badge covers us.*

Those are audits with a defined scope. Check
what is actually inside that scope.

5 *GDPR and HIPAA come included.*

GDPR needs a DPA. HIPAA needs a signed
BAA. Neither is automatic with a subscription.

AI adoption is a governance decision, not a purchase.

Govern by the terms and settings actually in use, not the name on the plan. Know where each type of data is allowed to go before your team uploads it.



FIND YOUR TOOLS · CHECK YOUR STATUS

Which of your AI tools are already covered?

 Covered by terms  Check the setting  Keep company data out

ChatGPT · OpenAI

Free / Plus / Pro (personal)	Consumer terms; training is a setting	 Check
Team	Commercial terms; not trained on by default	 Covered
Enterprise	Commercial terms + DPA	 Covered

Claude · Anthropic

Free / Pro (personal)	Consumer terms; training is a setting	 Check
Team / Enterprise / API	Commercial terms; not trained on by default	 Covered

Copilot · Microsoft

Personal account	Consumer terms	 Keep out
Work / school M365 (incl. 365 Copilot)	Your org's tenant boundary	 Covered

Gemini · Google

Personal / Advanced	Consumer terms; training is a setting	 Check
Workspace Business / Enterprise	Admin-governed Workspace terms	 Covered

“Covered” means the terms are in your favour, not that every job is cleared.

For regulated data, confirm the DPA and, for health data, a signed BAA. Status is set by how you access the tool, not the price of the plan. Verify current terms — they change often.