

Building Trust in AI and Privacy

IAPP PSR + AI Governance Global 2026 · Alea Garbagnati · Sabrina Ross · Polina Zvyagina · Lauren Wu

THE LIFECYCLE · FIVE STAGES, ONE CRAFT

- I TERROIR** *Provenance & consent*
Where it came from, and who said yes to what. No amount of skill downstream fixes fruit you should not have picked.
- II SORTING** *Minimization & quality*
What you deliberately leave behind. Nobody ferments everything they picked — what you drop determines what the finished thing tastes like.
- III THE CELLAR** *Access & retention*
Who holds the key, and when the window closes. A lock and a log, not just a door.
- IV THE LABEL** *Transparency & audit*
What you promised, and who verifies it. The inspection exists so the label means something.
- V THE POUR** *Reuse & translation*
What you actually serve, to whom, and how much. If you cannot explain it in two sentences, you have not simplified it.

FOUR DECISION TOOLS · USE THESE IN THE ROOM, NOT AFTER IT

THE FOUR PROVENANCE QUESTIONS

For sourcing

Where did it come from? Who said yes, and to what? Can we prove both? What did we promise?

If you cannot answer all four, you have a sourcing decision to revisit — not a documentation problem.

THE CELLAR TEST

For access

Who can reach it, why, for how long — and who checks?

A program that can answer the first three but not the fourth does not have access control. It has a door.

THE DRINKING WINDOW

For retention

Business-purpose end date? Legal floor underneath it? Risk of holding past both?

If the only honest answer to why you still have it is that deleting it is hard, you already have your answer.

THE POUR TEST

For communication

Can you explain it in two sentences to a non-lawyer — and would they make the same call?

If not, you have not simplified it. You have hidden it.

Ten translations for the people who fund you

Each of these is a translation device for a stakeholder with no legal or technical background. Take two. Use them instead of the vocabulary.

Provenance *is the label.*

If you cannot say where it came from, you cannot sell it — and increasingly you cannot lawfully use it either.

Minimization *is sorting the fruit.*

Nobody ferments everything they picked. What you leave out determines what the finished thing tastes like.

Retention *is the drinking window.*

Holding past peak is not prudence. It is an unrecognised liability sitting quietly in your cellar.

Access control *is a lock and a log.*

The question is never only who can get in. It is who checks who got in.

Purpose limitation *is what the bottle was bought for.*

A wine laid down for an anniversary is not automatically available for the cooking pot. "We already had it" has now been priced by a regulator.

Training data *is a blend.*

Once it is in, you cannot unblend it — which is why the decision that matters happens before it goes in the tank.

A risk assessment *is tasting before you bottle.*

Doing it after deployment is not an assessment. It is a recall.

An audit *is the appellation inspection.*

It exists so the label means something. Programs that treat it as an attack misunderstand what they are selling.

Over-collection *is over-extraction.*

Too much tannin and nobody can drink it — including you.

Deletion *is pouring it out.*

It always feels like waste. It is almost always the right call.

THE CLOCK THAT IS ALREADY RUNNING • CALIFORNIA

1 Jan 2027	ADMT compliance obligations take effect	31 Dec 2027	Pre-2026 processing must be risk-assessed
1 Apr 2028	First risk-assessment filings due	2028 → 2030	Cybersecurity audit certifications phase in by revenue

Do one thing this month: run the four provenance questions on the one system you are least sure about.