Is your LMS built for privacy, or just marketed that way?

8 Architecture questions you should ask to find out

QUESTION #1

What data categories does your contract explicitly prohibit?

What good looks like: A named list (government identifiers, protected health information, GDPR special categories) that is contractually binding, not just a policy statement.

If the answer is "we rely on customers to manage that," the vendor has no outer boundary on what enters their system.

QUESTION #2

If a single privileged credential were compromised, what is the maximum blast radius? One institution's data, or all of them?

What good looks like: Each institution's data should be logically isolated at the tenant level so that an application-layer compromise is scoped to one client. Ask specifically whether tenant isolation is enforced at the database layer or only at the application layer.

QUESTION #3

Does your platform use learner or course data to train, fine-tune, or improve your AI models?

What good looks like: An explicit "no" backed by contractual language.

Bonus: Ask whether data is used in any RAG system, and whether that data is deleted at contract termination.

QUESTION #4

Can you produce a complete inventory of what data your platform stores, in what form, and for how long?

What good looks like: A vendor who can answer this quickly has documented their data model.

A vendor who can't, has a massive breach waiting to happen. Look for a published DPIA or equivalent.

QUESTION #5

What third-party systems have access to learner data, and how are you notified when that list changes?

What good looks like: A published subprocessor list, advance notice of changes, and a contractual right to object.

The Canvas breach had a third-party integration as its known precursor. Every integration is an attack surface.

QUESTION #6

What happens to our data the day our contract ends?

What good looks like: Data is returned in a portable format and then deleted, including backups, within a defined window.

"We retain it for a while" is not an acceptable answer.

QUESTION #7

Where is our data hosted, and what governs cross-border transfers?

What good looks like: Customer-selectable regions with documented legal transfer mechanisms (SCCs, Data Privacy Framework).

If the vendor can't tell you where your data lives, they can't tell you who has jurisdiction over it.

QUESTION #8

What is your contractual breach notification commitment, and does it meet the 72-hour GDPR standard?

What good looks like: A specific timeline in the DPA.

Not "promptly" or "without undue delay" in a policy document, but a committed SLA in a contract you've signed.