

Four questions for an AI software supplier

To send to the supplier before signing, and again at every renewal. The Italian cybersecurity agency's FAQ says contract clauses alone are not enough: for every question, ask for evidence, not the brochure.

01 Clauses

WHAT TO ASK

- Which clauses cover security, subcontracting, and termination of the service.
- Within how many hours an incident touching our data is notified.
- No training on our data, written into the contract.
- Governing law and jurisdiction.

EVIDENCE TO RECEIVE

☐ Contract or security annex with written notification deadlines

☐ Exit clause with data return and formats

☐ No-training clause

Received on _____ · Assessment: adequate · to complete · not adequate

02 Evidence

WHAT TO ASK

- Which proof shows the measures exist, beyond the clauses.
- Certifications (ISO 27001 or equivalent) and their scope.
- Security test results from the last twelve months.
- An operations log the customer can consult.

EVIDENCE TO RECEIVE

☐ Certificate with scope and body

☐ Test summary with date and outcome

☐ Sample log extract

Received on _____ · Assessment: adequate · to complete · not adequate

03 Second-tier dependencies

WHAT TO ASK

- Where the models run and who provides the infrastructure.
- In which country the data sits at rest and in transit.
- Who else can access it: subcontractors, support, development.
- What happens if a subcontractor revokes the service.

EVIDENCE TO RECEIVE

☐ List of subcontractors with role and country

☐ Data flow diagram

☐ Subcontractor contracts covering points 01 and 02

Received on _____ · Assessment: adequate · to complete · not adequate

04 Replaceability

WHAT TO ASK

- What stays with the company at contract end: data, rules, configurations, know-how.
- In which formats and within how many days.
- Whether the model can be swapped without losing the context.
- What happens to the factory if the license is revoked.

EVIDENCE TO RECEIVE

☐ Export procedure with formats

☐ Export test on a sample

☐ Open-formats statement

Received on _____ · Assessment: adequate · to complete · not adequate

Supplier response form

Filled in and signed by the supplier. Every answer points to an attached document; an answer without an attachment counts as not given. Yempik fills in this form for its own clients before any proposal.

Supplier

Contact

Date

01

Clauses

Incident notification within hours (clause no.)

No training on customer data: yes · no (clause no.)

Exit and data return within days, formats

Governing law · jurisdiction

02

Evidence

Certification · body · expiry · scope

Last security test: date · outcome · attachment no.

Operations log: where · who reads it · retention months

03

Second-tier dependencies

SUBCONTRACTOR	ROLE	COUNTRY	DATA PROCESSED

Model execution: inside the customer perimeter · dedicated EU cloud · public cloud (country)

Data at rest in · data in transit

04

Replaceability

What is returned: data · rules · configurations · log · other

Formats · time days · cost

Model swap without losing the context: yes · no · how

Supplier signature · Company security officer signature