VendoCerta

VENDOCERTA MATERIALS

Security & GDPR

Data protection in VendoCerta is spread across the product: in how the trail is recorded, in who may see which document, in how a bank account is encrypted, and in what a role deliberately cannot do. This page gathers it in one place — including the parts where the honest answer is “not yet”.

5	5	AES-256
roles with separated duties	rules no role can bypass	sensitive-data encryption

Generated: 2026-08-21

vendocerta.com

VENDOCERTA

Six questions that come up first.

Can the data stay with us?

Yes. VendoCerta installs on infrastructure you control.

How is sensitive data protected?

AES-256-GCM at rest; revealing it requires a re-entered password and a reason logged to the trail.

Who has access to what?

Roles with genuine separation of duties. Nobody can change their own role.

Is there a second factor at sign-in?

Yes, mandatory for roles with access to business data.

Can one person change a supplier's bank account?

No. Four stages, separated roles, a minimum of two people.

Can the audit trail be corrected?

No. There is no edit or delete function in the interface, in any role, not even for the owner.

An entry cannot be changed or deleted. Not even by the owner.

Every recorded action becomes an entry: a sign-in, a supplier status change, a document decision, an invitation sent, a file downloaded. VendoCerta has no function anywhere to edit or delete one, and never overwrites an existing event.

Before and after, on every data change

Each entry carries who, what, when — and for a change, what the values looked like on both sides of it.

Refusals are recorded too

If somebody tries to open something they have no permission for, that attempt is an entry. Repeated attempts are therefore visible rather than silent.

A filtered view is a link

Filters go into the page address, so a specific slice of the trail can be handed to a colleague — or an auditor — as a URL. That is exactly how a single case links to its own history.

Its own retention, and we say so

The number of days at the foot of the audit screen is not the field on the settings screen. Audit retention is a separate setting that cannot currently be changed from the interface, and changing the other one will not move it.

The one operation the product refuses to make convenient.

Changing a supplier’s bank account is four stages and a rule about who may finish them. Everything else in VendoCerta is designed to remove friction; this is designed to keep it.

Encrypted the moment it is saved

An account number is never plain text in the database — AES-256-GCM at rest, from the moment it is stored.

Revealing it costs three things

The sensitive-data permission, your password again even though you are signed in, and a stated reason recorded in the trail. The reason is recorded; the number never is. It clears from the screen after 45 seconds.

Duplicates are surfaced, not hidden

If the same account number already sits against another supplier, the warning has to be knowingly dismissed before approval becomes possible at all.

Five roles, and the surprising one is deliberate.

The system administrator keeps the installation running — configuration, diagnostics, backups — and has no visibility into suppliers, documents, cases or bank accounts at all. The exact opposite of the business administrator, who runs the supplier side and cannot restore a backup.

CAPABILITY	OWNER	BUSINESS ADMINISTRATOR	SYSTEM ADMINISTRATOR	REVIEWER	OBSERVER
Sees suppliers and documents	✓	✓	–	✓	✓
Adds and edits suppliers	✓	✓	–	–	–
Reviews documents and decides on approval	✓	✓	–	✓	–
Sees sensitive documents (payment details)	✓	✓	–	–	–
Manages users and roles	✓	✓	✓	–	–
Restores a backup	✓	–	–	–	–

The rules a role cannot talk its way around

- Nobody — including the owner — can change their own role.
- An administrator cannot create, or demote, an account holding the owner role.
- The last remaining owner account cannot be demoted or disabled, so a company is never left with nobody in charge of it.
- Two-factor authentication is mandatory and unskippable for owner, business administrator, system administrator and reviewer. An observer may switch it on but does not have to.
- A failed sign-in never says whether it was the e-mail or the password, so the screen cannot be used to discover whether an account exists.

What is held, who can reach it, and for how long.

Sensitive documents need their own permission

Ordinary supplier documents are visible to anyone with access to the record. Documents marked sensitive — chiefly payment-related — need a separate permission on top, which in practice means owner and administrator only. Trying to open one without it produces a refusal, and the refusal is recorded.

Files are never a permanent URL

A download goes through a digitally signed link valid for a few minutes and tied to your own company. Opening it from another context gets nowhere. Every download of a sensitive file is audited separately.

Retention: seven years by default

The documents-and-retention setting defaults to 2,555 days, matching typical procurement audit requirements, and can be changed at any time. Honestly: today it records your policy and will drive future housekeeping — nothing is deleted automatically because the date passed.

Invitations expire, and reissuing revokes

An invitation link is a single-use random token with a limited life, a week by default. Sending a new invitation invalidates the previous one immediately, even if somebody had opened it — and that is currently the only way to cut a link off; there is no separate revoke button.

Bank details encrypted at rest

AES-256-GCM from the moment of saving. The stated reason for revealing a number goes into the audit trail; the number itself never does.

A support report that carries no data

The diagnostics tab of the system centre produces a report for technical support containing versions, counts and masked log lines — never document contents, banking details or suppliers' personal data.

The questions an assessor sends first.

Is VendoCerta a cloud service we are trusting with our data?

No. It installs onto a machine you control. PostgreSQL, object storage and the mail preview run as portable binaries inside the project folder — nothing installed into Windows, no administrator rights, Docker optional. Internet access is needed on first run to fetch those services, and after that the installation is yours.

Can we get technical documentation beyond this page?

Yes. The installation ships with the security model and threat model as documents in the repository — the same sources this page is drawn from. Ask whoever maintains your installation, or ask us on the demo form and say it is for a security review.

What does the AI assistant have access to?

Only what the person asking may already see, and it never carries out an action without that person’s explicit confirmation — permissions are re-checked at the moment of the click, against the person clicking. It cannot approve, reject or suspend a supplier, cannot change a role, and cannot delete anything.

Does a password reset get somebody past two-factor authentication?

No. For the roles where the second factor is mandatory it is mandatory on every route into the account, including after a reset.

Where are e-mails sent during a pilot?

Into a local preview inbox on the installation itself, not to real recipients — so a pilot cannot accidentally e-mail a supplier. The system centre’s installation tab says which mailbox an installation is actually using.