NOVA Invoice Suite · Key To Business S.r.l.

SECURITY · COMPLIANCE · DATA PROTECTION

The controls an auditor asks about, and where each one is applied

Authorisation, evidence, personal data and retention — described as mechanisms with a location in the product, not as assurances. Where a control is the customer’s responsibility, that is stated too.

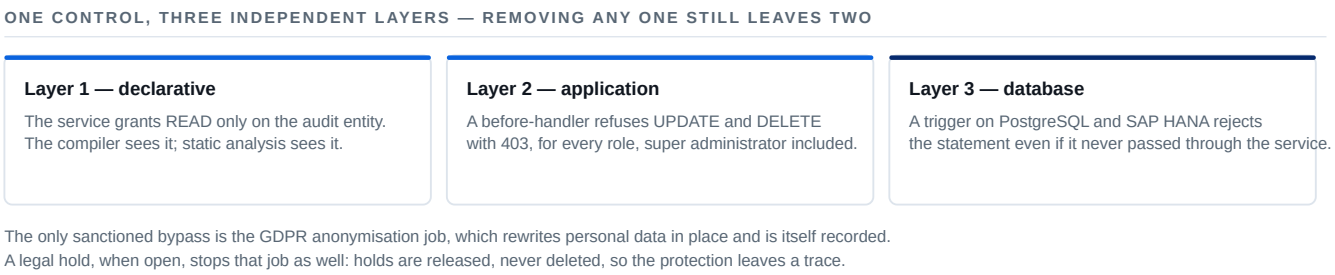
1.0.0	2026-09-10	15 canonical	Single tenant per customer
Version	Date	Roles	Tenancy

Authorisation

15 canonical roles are expressed as authorisation scopes with a company-code attribute, declared in the security descriptor and enforced declaratively in the service model — which means the compiler and static analysis see them, not only the runtime. Operational work, approval and posting are **mutually exclusive**: the same person cannot process an invoice, approve it and post it. One combined role exists for small organisations where that separation is impractical; it is documented as an exemption and intended for periodic review, rather than being an undeclared hole.

Every entity carrying a company code is scoped to the user's own company. Only the super administrator crosses that boundary, and **every cross-company query a super administrator performs is written to the audit trail**.

Evidence that survives



The only sanctioned bypass is the GDPR anonymisation job, which rewrites personal data in place and is itself recorded. A legal hold, when open, stops that job as well: holds are released, never deleted, so the protection leaves a trace.

Defence in depth is the rule for every control of this grade: at least two independent layers, ideally three. A single layer is accepted only where a bypass is not plausible.

Personal data

CONTROL	HOW IT WORKS
Classification	The data model is annotated with the SAP @PersonalData vocabulary: field-level classifications distinguishing potentially personal from potentially sensitive, plus field semantics. The annotations are the authoritative source — a list rewritten by hand elsewhere would diverge.
Masking in the audit trail	Every textual field written to the audit trail passes through a sanitiser that masks Italian IBANs, tax codes, VAT numbers and e-mail addresses, preserving the last characters so a human can still recognise the record.
Masking towards AI models	Reversible personal-data masking is enforced in production in the AI orchestration client. The agent-facing service exposes read-only projections with the personal fields removed at the model level, so it is not a matter of trusting the caller.
Retention and destruction	The SAP Information Lifecycle Management vocabulary is adopted with SAP's own field names. The model separates the *residence* period, at whose end the record is blocked, from the *retention* period, at whose end it is destroyed. The anchor for the ten-year count is configurable, and the default is the fiscal-year-end reading of Italian law — the conservative one, because on a legal minimum an error in excess can still be corrected and an error in deficit cannot.
Legal hold	When a dispute or a tax audit is open, a hold scoped to a company code and optionally to a single invoice stops *both* destructive jobs — the purge and the anonymisation. Covering only one would leave the other free to destroy data under protection.

Data-subject reporting	The SAP Data Privacy Integration information service is supported through the official CAP plugin, opt-in and information-only.

> **Invoice data does not leave the customer's infrastructure.** NOVA is installed single-tenant inside the customer's own SAP account. Towards the data subjects the *customer* is the controller and issues the notice; the publisher acts as processor and does not access the data except on explicit and traced request, in a support context.

Content and transport

CONTROL	HOW IT WORKS
Malware scanning	SAP Malware Scanning Service on every document boundary, fail-closed. A daily canary proves the gate still answers, because the binding certificate has a finite life and a failed rotation would otherwise be discovered by the first rejected invoice.
Upload validation	The declared content type is never trusted on its own: the leading bytes of the file are verified against it.
Input bounds	Explicit caps on batch invoice bodies and on query expansion depth, and dedicated rate limits per surface — global, writes, uploads, scheduled-job endpoints, analytics consumers and machine interfaces.
Secrets	Configuration export masks secret fields on two independent criteria — an explicit flag and a name heuristic — so a new secret field is masked by default rather than by remembering. Service tokens are rotated quarterly, and immediately if one appears in a commit or a log.
Supply chain	Every third-party CI action is pinned by commit hash; dependency updates are automated; a gate refuses a dependency major that the runtime cannot support, because the package manager's own check is disabled in this project and a silent install is not a verification.

What remains the customer's responsibility

- Issuing the privacy notice to data subjects and holding the contract with the accredited preservation provider — both follow from the customer being the controller.
- Assigning roles to real people, and reviewing the combined operational role if it is used.
- Operating the identity provider, and the lifecycle of its trust with the platform.
- Deciding the retention anchor if a legal opinion prefers a reading other than the default.

> **What this document is not.** It describes mechanisms present in the product and where they are applied. It is not a certification, and it is not legal advice: the contractual data-processing terms and the privacy notice are separate documents, reviewed by a professional before publication.

NOVA Invoice Suite 1.0.0 · 2026-09-10 · Key To Business S.r.l. · Figures in this document are measured from the product repository by an automated gate, not transcribed by hand.