

Compliance with PaperOffice AI: workspaces, Audit Center, evidence

Who saw, changed, shared or deleted which document, and when? That record cannot be built after the fact. PaperOffice logs immutably, redacts personal data and enforces a retention period per document type.

Three security tiers per workspace

Standard

For everyday operations

- AES-256 chunk encryption of every file and RAM disk processing
- Whitelist access lists and roles
- Versions with audit trail, permanent deletion

For teams, projects and daily work

Business

For sensitive records

- Everything in Standard
- Recycle bin, WORM write protection and workspace password
- Access protection, external sharing, SMS or two-person approval

For accounting, HR and contracts

Compliance

For high security

- Everything in Business
- Hardware encryption
- IP whitelist, mandatory 2FA, watermarks and protected PDF delivery

For regulated industries and audits

How a compliance workspace is set up

- 1 Create**
Choose name, purpose and type: Standard, Business or Compliance. Plus processing depth from Archive to Ultra, storage location EU cloud or your own storage mount, retention period and language.
- 2 Secure**
Per workspace password, two-person or SMS approval, recycle bin, WORM protection, external shares with expiry, in Compliance additionally IP whitelist, mandatory 2FA, watermarks and hardware encryption.
- 3 Work**
Users and groups get permissions per workspace, agents and MCP respect them. Upgrading the level is possible any time, downgrading is not, for compliance reasons.

Audit Center

The audit center records who did what with which document and when, and rates findings by severity.

- 1 Record**
Every action on a document is captured with time, user, context and integrity hash: view, change, export, approve, delete. Not editable afterwards.
- 2 Rate**
The AI compares documents and actions with patterns and master data: differing bank account, arithmetic errors, unusual access. Every finding gets a severity from low to critical.
- 3 Review**
Critical findings trigger notifications and become a task for a reviewer: approve, reject or escalate, with a comment in the trail. Reports for auditors as PDF, CSV or JSON.

Complete trail

Every action with time, user, document and context, field-level on changes: old value, new value.

Immutable

Entries with integrity hash, not editable or deletable afterwards.

Export and reports

Audit report per document as PDF, trail as CSV or JSON, with selectable scope.

Retention

WORM protection and retention periods per document type, deletions themselves are part of the trail.

Retention, redaction, integrity

Retention per document type

A retention period in years per workspace, with WORM protection that stays in place once activated.

Approval as a process

Two-person approval, tasks with deadline and escalation, every step ends up in the log.

Three security levels

Standard, Business and Compliance with recycle bin, WORM, password, IP list and hardware encryption.

Trust Agent

The Trust Agent checks PDFs for hidden content, overlays, embedded files and manipulation.

Evidence and documents

DPA generator · Art. 28 GDPR

The data processing agreement is created in the app — pre-filled with the company data, as a PDF on PaperOffice letterhead.

Security Center

All devices and sessions of the account at a glance — who accesses what, when and from where.

ISO/IEC 27001 (certified)

International standard for Information Security Management. ISO/IEC 27001 certified (certificate available under NDA); SOC 2 Type II in preparation.

Operations and encryption

Data center

Documents in. Results out. No external AI providers, no AI subprocessors, and no training on your data. Own data center in the EU (Navarra, Spain).

Key Management

Keys stored outside the database — readable only by authorised services

PII found automatically

Names, addresses, IBANs, dates of birth, email and phone selectable per category, plus custom terms and a whitelist.

Integrity checked

Hidden text, covered areas, embedded files and multiple save states are made visible.

Redact Agent

The Redact Agent detects names, addresses, IBANs and other PII in documents and images and redacts them.

Audit-safe email delivery

Send up to ten documents from the DMS by email, with PDF password, secure link and a log of every step.

TOM generator · Art. 32 GDPR

Technical and organisational measures for exactly the services used in the account.

GDPR

PaperOffice meets the GDPR requirements for processors — DPA (Art. 28) and TOMs (Art. 32) from the generator, processing in the EU.

SOC 2 Type II (in preparation)

AICPA Service Organization Control for Trust Services Criteria

Encryption

AES-256 at rest, every file encrypted chunk by chunk, TLS 1.3 in transit, Compliance workspaces additionally with hardware encryption.

Access control

Decryption only for authorized processing – with audit trail

Note. Whether a process meets regulatory requirements depends on the implementation in your company (roles, procedural documentation, controls). PaperOffice AI provides the technical building blocks; this datasheet does not replace legal advice. Evidence: ISO/IEC 27001 certified (certificate available under NDA); SOC 2 Type II in preparation.